SIEMENS

SIMATIC

# Industrie Software Safety Matrix

Projektierungshandbuch




02/2010

A5E00265324-03

## Rechtliche Hinweise

### Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

| ⚠GEFAHR |
| --- |
| bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden. |

| ⚠WARNUNG |
| --- |
| bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden. |

| ⚠VORSICHT |
| --- |
| mit Warndreieck bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden. |

| VORSICHT |
| --- |
| ohne Warndreieck bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden. |

| ACHTUNG |
| --- |
| bedeutet, dass ein unerwünschtes Ergebnis oder Zustand eintreten kann, wenn der entsprechende Hinweis nicht beachtet wird. |

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

### Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

### Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

| ⚠WARNUNG |
| --- |
| Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden. |

### Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

### Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

A5E00265324-03
℗ 02/2010

# Vorwort

## Vorwort

### Zweck der Dokumentation

Die Informationen dieses Handbuchs ermöglichen es Ihnen, fehlersichere Systeme S7 F/FH Systems mithilfe der *Safety Matrix* V6.2 zu projektieren.

Ergänzend benötigen Sie

- das Systemhandbuch "Sicherheitstechnik in SIMATIC S7 (http://support.automation.siemens.com/WW/view/de/12490443)" und
- das Programmier- und Bedienhandbuch "S7 F/FH Systems, Projektieren und Programmieren (http://support.automation.siemens.com/WW/view/de/2201072)".

### Erforderliche Grundkenntnisse

Zum Verständnis dieser Dokumentation werden allgemeine Kenntnisse auf dem Gebiet der Automatisierungstechnik vorausgesetzt. Außerdem sind Grundkenntnisse auf folgenden Gebieten erforderlich:

- fehlersichere Automatisierungssysteme
- Automatisierungssysteme S7-400H
- S7 F/FH Systems
- dezentrale Peripheriesysteme am PROFIBUS DP
- Basissoftware *STEP 7 / PCS 7*, insbesondere:
  - Umgang mit dem *SIMATIC Manager*
  - Hardwarekonfiguration mit *HW Konfig*
  - Kommunikation zwischen CPUs
  - Optionssoftware *CFC*
  - *PCS 7* (für *Safety Matrix Viewer*)

## Gültigkeitsbereich der Dokumentation

| Optionspaket | Bestellnummer | ab Erzeugnisstand | Lizenz |
|---|---|---|---|
| Optionspaket *Safety Matrix Editor* inklusive Autorisierungslizenz | • 6ES7833-1SM42-0YA5 | V6.2 | Single, Trial (1 Monat) |
| Optionspaket *Safety Matrix Engineering Tool* inklusive Autorisierungslizenz | • Vollversion: 6ES7833-1SM02-0YA5 | V6.2 | Floating, Trial (14 Tage) |
| | • Upgradeversion von V5.2 oder V6.1: 6ES7833-1SM02-0YE5 | | Floating (als Upgrade), Trial (14 Tage) |
| Optionspaket *Safety Matrix Viewer* inklusive Autorisierungslizenz | • Vollversion: 6ES7833-1SM62-0YA5 | V6.2 | Floating, Trial (14 Tage) |
| | • Upgradeversion von V5.2 oder V6.1: 6ES7833-1SM62-0YE5 | | Floating (als Upgrade), Trial (14 Tage) |

Die Optionspakete der *Safety Matrix* dienen dem Safety Lifecycle-Engineering und – Management für die fehlersicheren Automatisierungssysteme S7 F/FH Systems und unterstützen in allen Phasen des Safety Lifecycle.

## Änderungen gegenüber der Vorgängerversion

- Beschreibung der folgenden wichtigen Neuerungen:
  - Überarbeitung/Erweiterung der Benutzeroberfläche
  - Überarbeitung der TAG-Eingabe
  - Vorverarbeitung für Cause-TAGs
  - Erweiterungen für Causes (Vorwarnung für Analogwerte, Wert simulieren mit gegenseitiger Verriegelung, Effect-TAG als interne Referenz)
  - Erweiterte Einstellungsmöglichkeiten für die Kanaltreiber
  - Einbeziehen von kundenspezifischen F-Kanaltreibern
  - Erweiterungen für Effects (Wert simulieren mit gegenseitiger Verriegelung, Vorwarnung für Übersteuern-Timeout)
  - Verdoppelung der möglichen *Safety Matrix*-Schnittpunkte auf 1024
  - Erweiterungen für Bedienen und Beobachten (Wartungsänderungen, Statusfarben)
  - Einstellbare Farben
  - Farbliche Darstellung einzelner TAGs im Online-Betrieb
  - Überarbeitung / Erweiterung des Alarmverhaltens mit drei neuen Funktionsblöcken für Alarme (F_SC_AL, F_SE_AL, F_MA_AL) und drei neuen Safety Matrix-Bausteinsymbolen zur Bedienung
  - Selektive Darstellung der Safety Matrix im *Safety Matrix Viewer*: einzelner Cause mit den dazugehörigen Effects; einzelner Effect mit den dazugehörigen Causes
  - Handling mehrerer Safety Matrizen mit unterschiedlichen Versionen in derselben *PCS 7*-OS

## Approbationen

Die *Safety Matrix*-Optionspakete sind zertifiziert für den Einsatz im Sicherheitsbetrieb bis:

- Sicherheits-Integritätslevel (Safety Integrity Level) SIL3 nach IEC 61508
- Kategorie 4 nach EN 954-1
- Performance Level (PL) e nach ISO 13849-1:2006 bzw. nach EN ISO 13849-1:2008

## Einordnung in die Informationslandschaft

Für die Arbeit mit der Safety Matrix benötigen Sie je nach Anwendungsfall zusätzliche, nachfolgend aufgeführte Dokumentationen.

In der vorliegenden Dokumentation wird an geeigneten Stellen auf diese Dokumentationen verwiesen.

Beachten Sie darüber hinaus die FAQs unter:
(http://support.automation.siemens.com/WW/view/de/26091998/133000)

| Dokumentation für | Relevante Inhalte in Kurzform |
|---|---|
| S7 F/FH Systems | • Das Programmier- und Bedienhandbuch "S7 F/FH Systems, Projektieren und Programmieren (http://support.automation.siemens.com/WW/view/de/2201072)" beschreibt die Projektierung und Programmierung von fehlersicheren Systemen S7 F/FH Systems mithilfe von *S7 F Systems*.<br>• Das Installationshandbuch "Automatisierungssysteme S7-400, Aufbauen (http://support.automation.siemens.com/WW/view/de/1117849)" beschreibt die Montage und Verdrahtung von Systemen S7-400.<br>• Das Handbuch "Automatisierungssystem S7-400H, Hochverfügbare Systeme (http://support.automation.siemens.com/WW/view/de/1186523)" beschreibt die Zentralbaugruppen CPU 41x-H und die auszuführenden Aufgaben, um ein hochverfügbares System S7-400H zu erstellen und in Betrieb zu nehmen. |
| Sicherheitstechnik in SIMATIC S7 | Das Systemhandbuch "Sicherheitstechnik in SIMATIC S7 (http://support.automation.siemens.com/WW/view/de/12490443)" vermittelt Überblickswissen zu Einsatz, Aufbau und Funktionsweise von fehlersicheren Automatisierungssystemen S7 Distributed Safety und S7 F/FH Systems und beschreibt grundlegende Eigenschaften und technische Detailinformation zu diesen fehlersicheren Systemen. |
| *STEP 7*-Handbücher | • Das Handbuch "Hardware konfigurieren und Verbindungen projektieren mit STEP 7 V5.4 (http://support.automation.siemens.com/WW/view/de/18652631)" beschreibt die Bedienung der entsprechenden Standard-Tools von *STEP 7*.<br>• Das Referenzhandbuch "Systemsoftware für S7 300/400 System- und Standardfunktionen (http://support.automation.siemens.com/WW/view/de/1214574)" beschreibt Funktionen für Zugriff/Diagnose der dezentralen Peripherie/CPU.<br>• Das Handbuch/die Online-Hilfe "CFC für S7 Continuous Function Chart (http://support.automation.siemens.com/WW/view/de/21401430)" beschreibt die Programmierung mit *CFC*.<br>• Das Handbuch "Anlagenänderung im laufenden Betrieb mittels CiR (http://support.automation.siemens.com/WW/view/de/14044916)" |

| Dokumentation für | Relevante Inhalte in Kurzform |
| --- | --- |
| *STEP 7*-Onlinehilfe | • beschreibt die Bedienung der Standard-Tools von *STEP 7*<br>• enthält Informationen zum Konfigurieren und Parametrieren von Peripherie mit *HW Konfig* |
| *PCS 7* | Die *PCS 7*-Handbücher beschreiben die Handhabung des Leitsystems *PCS 7* (notwendig, wenn das S7 F-System in ein übergeordnetes Leitsystem eingebunden wird):<br>• Projektierungshandbuch "Engineering System (http://support.automation.siemens.com/WW/view/de/27002802)"<br>• Projektierungshandbuch "Hochverfügbare Prozessleitsysteme (http://support.automation.siemens.com/WW/view/de/27002533)"<br>• Projektierungshandbuch "Operator Station (http://support.automation.siemens.com/WW/view/de/27002758)"<br>• Bedienhandbuch "PC-Konfiguration und Autorisierung (http://support.automation.siemens.com/WW/view/de/27002558)" |

## Wegweiser

Die vorliegende Dokumentation beschreibt den Umgang mit den Optionspaketen *Safety Matrix Engineering Tool*, *Safety Matrix Viewer* und *Safety Matrix Editor*. Sie besteht aus anleitenden Kapiteln und Kapiteln zum Nachschlagen (Beschreibung der Parametrierungsmöglichkeiten).

Die Dokumentation beinhaltet die folgenden Themen:

- Projektieren des Sicherheitsprogramms (sicherheitsgerichtetes Anwenderprogramm) für S7 F/FH Systems
- Transferieren, Übersetzen und Laden der Safety Matrix
- Zugriffschutz für die Safety Matrix
- Bedienen und Beobachten in *PCS 7*
- Unterstützung bei der Abnahme der Anlage

## Konventionen

In der vorliegenden Dokumentation werden die Begriffe "Sicherheitstechnik" und "F-Technik" synonym verwendet. Genauso wird mit den Begriffen "fehlersicher" und "F-" verfahren.

Der hier verwendete Begriff "Projektieren" entspricht dem in referenzierten Dokumentationen verwendeten "Programmieren".

*"S7 F Systems"* in kursiver Schreibweise bezeichnet das Optionspaket für das fehlersichere System "S7 F/FH Systems".

Der Begriff "Sicherheitsprogramm" bezeichnet den fehlersicheren Teil des Anwenderprogramms und wird anstelle von "fehlersicheres Anwenderprogramm", "F-Programm", etc. verwendet. Zur Unterscheidung wird das nicht sicherheitsgerichtete Anwenderprogramm als "Standard-Anwenderprogramm" bezeichnet.

"F-CPU" bezeichnet eine F-fähige CPU. Eine F-fähige CPU ist eine Zentralbaugruppe, die für den Einsatz in S7 F/FH Systems zugelassen ist.

## Weitere Unterstützung

Bei Fragen zur Nutzung der im Handbuch beschriebenen Produkte, die Sie hier nicht beantwortet finden, wenden Sie sich bitte an Ihren Siemens-Ansprechpartner in den für Sie zuständigen Vertretungen und Geschäftsstellen.

Ihren Ansprechpartner finden Sie im Internet (http://www.siemens.com/automation/partner).

Den Wegweiser zum Angebot an technischen Dokumentationen für die einzelnen SIMATIC-Produkte und Systeme finden Sie im Internet (http://www.siemens.de/simatic-tech-doku-portal).

Den Online-Katalog und das Online-Bestellsystem finden Sie im Internet (http://mall.automation.siemens.com).

## Trainingscenter

Um Ihnen den Einstieg in das Automatisierungssystem *SIMATIC S7* zu erleichtern, bieten wir entsprechende Kurse an. Wenden Sie sich an Ihr regionales Trainingscenter oder an das zentrale Trainingscenter in D 90327 Nürnberg.

Weitere Informationen erhalten Sie im Internet (http://www.sitrain.com).

## H/F Competence Center

Zu den Themen fehlersichere und hochverfügbare Automatisierungssysteme *SIMATIC S7* bietet das H/F Competence Center in Nürnberg spezielle Workshops an. Außerdem hilft Ihnen das H/F Competence Center bei der Projektierung, bei der Inbetriebsetzung und bei Problemen vor Ort.

Anfragen zu Workshops usw. richten Sie an: hf-cc.aud@siemens.com

## Technical Support

Sie erreichen den Technical Support für alle Industry Automation-Produkte über das Web-Formular (http://www.siemens.com/automation/support-request) für den Support Request.

Weitere Informationen zu unserem Technical Support finden Sie im Internet (http://www.siemens.com/automation/service).

## Service & Support im Internet

Zusätzlich zu unserem Dokumentationsangebot bieten wir Ihnen im Internet (http://www.siemens.com/automation/service&support) unser komplettes Wissen online an.

Dort finden Sie:

- den Newsletter, der Sie ständig mit den aktuellsten Informationen zu Ihren Produkten versorgt.
- die für Sie richtigen Dokumente über unsere Suche in Service & Support.
- ein Forum, in welchem Anwender und Spezialisten weltweit Erfahrungen austauschen.
- Ihren Ansprechpartner für Industry Automation-Produkte vor Ort über unsere Ansprechpartner-Datenbank.
- Informationen über Vor-Ort-Service, Reparaturen, Ersatzteile und vieles mehr stehen für Sie unter dem Begriff "Reparaturen, Ersatzteile und Consulting" bereit.

## Wichtiger Hinweis für die Erhaltung der Betriebssicherheit Ihrer Anlage

**Hinweis**

Anlagen mit sicherheitsgerichteter Ausprägung unterliegen seitens des Betreibers besonderen Anforderungen an die Betriebssicherheit. Auch der Zulieferer ist gehalten, bei der Produktbeobachtung besondere Maßnahmen einzuhalten. Wir informieren deshalb in einem speziellen Newsletter über Produktentwicklungen und -eigenschaften, die für den Betrieb von Anlagen unter Sicherheitsaspekten wichtig sind oder sein können. Damit Sie auch in dieser Beziehung immer auf dem neuesten Stand sind und ggf. Änderungen an Ihrer Anlage vornehmen können, müssen Sie den entsprechenden Newsletter abonnieren. Gehen Sie dazu ins Internet (https://www.automation.siemens.com/WW/newsletter/guiThemes2Select.aspx?HTTPS=REDIR&subjectID=2).

Melden Sie sich dort für folgende Newsletter an:

- S7-300 / S7-300F
- S7-400 / S7-400H / S7-400F/FH
- Dezentrale Peripherie
- SIMATIC Industrie Software

Aktivieren Sie bei diesen Newslettern jeweils das Kästchen "Aktuell".

## Verzeichnis der Warnhinweise

| Warnung | Kapitel |
|---|---|
| Warnhinweise des Programmier- und Bedienhandbuchs "S7 F/FH Systems" | 1.1 |
| Sicherer Zustand bei digitaler F-Peripherie | 1.4 |
| Betrieb der Safety Matrix | 2.1 |
| Installierte Version der Safety Matrix-Komponenten prüfen | 2.2 |
| Geben Sie einer Safety Matrix einen eindeutigen Namen | 3.1 |
| Bearbeiten der Safety Matrix-Datei | 3.2 |
| Zuordnung der Farben | 4.2.2 |
| Auswirkung auf Änderungsladen | 6.1 |
| Transfer mit Option "Plan + Parameter" | 6.1 |
| Hierarchischer Plan der Kanaltreiber | 6.1 |
| Hierarchischer Plan der Matrixlogik | 6.1 |
| Safety Matrix-Basisplan | 6.1 |
| Warn- und Sicherheitshinweise des Benutzerhandbuchs zur *Safety Matrix* V5.2 | 8.1 |
| Unabhängige Wege zur Anzeige | 8.1 |
| Standard-Bediener | 8.5 |
| Durch die Funktionalität "Secure Write" werden Änderungen im RUN am Sicherheitsprogramm vorgenommen | 8.5.2.1 |
| Bedienen einer Safety Matrix | 8.5.2.1 |
| Secure Write: Korrekte Funktion der Bedienung prüfen | 8.5.2.1 |
| Prüfen einer Transaktion | 8.5.2.1 |
| Prüfen der technologischen Zuordnung | 8.5.2.1 |
| Abbruch einer Transaktion | 8.5.2.1 |
| Wiedereingliederung der F-Kanaltreiber | 8.5.3.1 |

# Inhaltsverzeichnis

# Produktübersicht 1

## 1.1 Was ist die Safety Matrix?

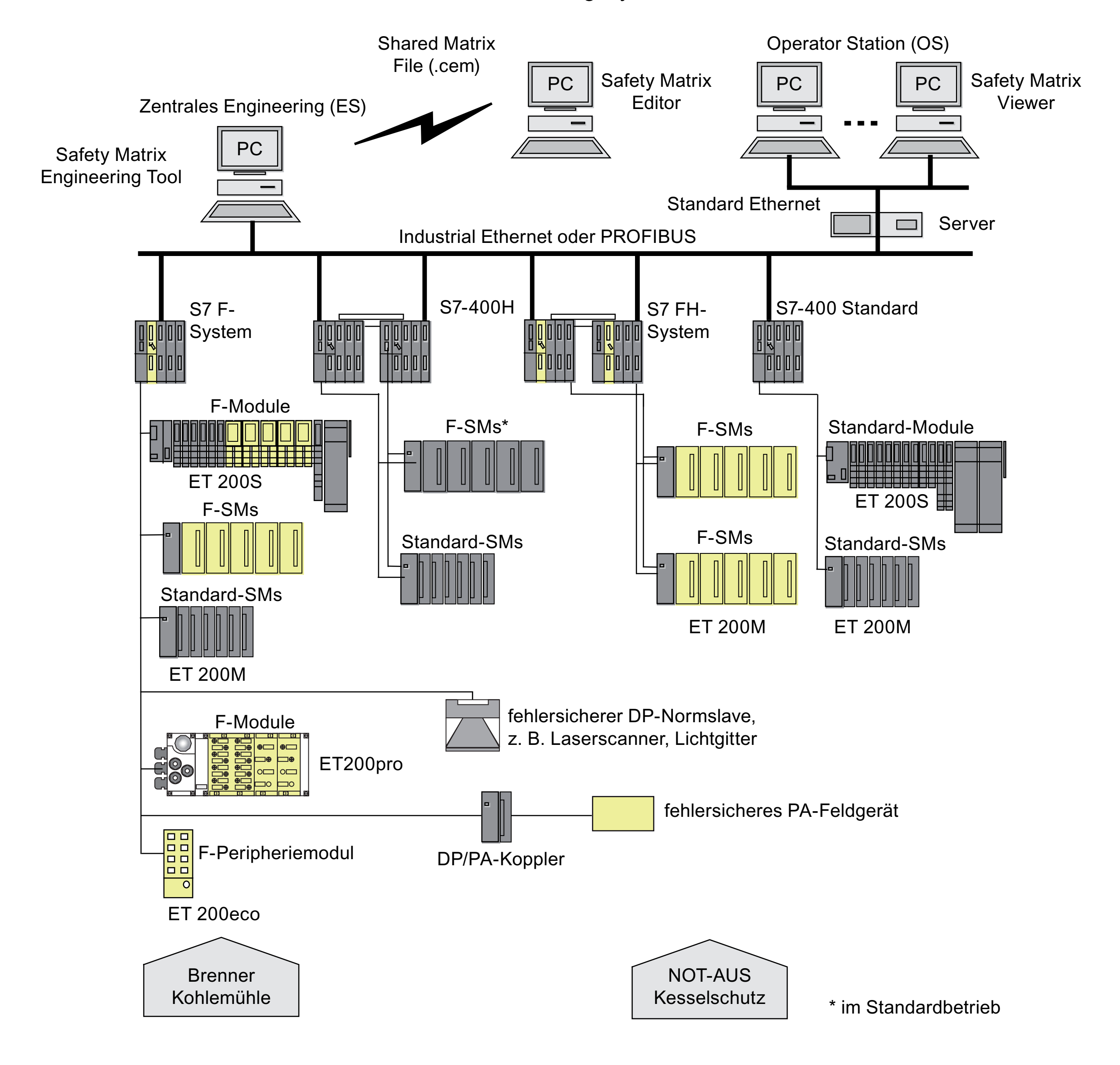
### Umfassendes Tool für Safety Lifecycle

Die SIMATIC *Safety Matrix* ist das umfassende Tool für Safety Lifecycle-Engineering und –Management für die fehlersicheren Automatisierungssysteme S7 F/FH Systems und unterstützt in allen Phasen des Safety Lifecycle:

- Die *Safety Matrix* ist ein Projektierungstool für Prozesse, die Sicherheitsreaktionen auf definierte Zustände erfordern.
- Mit der *Safety Matrix* kann ein *CFC*-Sicherheitsprogramm für S7 F/FH Systems nach den Regeln einer Cause/Effect-Matrix (Ursache/Wirkungs-Matrix) erstellt werden.
- Die *Safety Matrix* ist ein integriertes Tool für alle Abläufe, Wartung, Fehlerbehandlung und Änderungsmanagement während des Betriebs.

## Einsatz in der Prozesstechnik

Das folgende Bild zeigt Ihnen Integrationsmöglichkeiten von S7 F/FH Systems mit der *Safety Matrix* in Ihr Prozessautomatisierungssystem mit *PCS 7*.



## Bezug zu *S7 F Systems*



**WARNUNG**

**Warnhinweise des Programmier- und Bedienhandbuchs "S7 F/FH Systems"**

Die *Safety Matrix* ist ein Optionspaket für S7 F/FH Systems. Sie müssen alle Warnhinweise im Programmier- und Bedienhandbuch "S7 F/FH Systems, Projektieren und Programmieren" lesen, verstehen und beachten.

Die folgende Tabelle veranschaulicht den Bezug zwischen der *Safety Matrix* und *S7 F Systems*.

| *S7 F Systems* | *Safety Matrix* |
|---|---|
| Programmieren im *CFC* | Intuitive Projektierung auf Basis der gängigen Cause/Effect-Methode |
| *CFC* als Basis (Pläne, Ablaufgruppen, Ablaufreihenfolge) | |
| *S7 F Systems*-Sicherheitskonzept | |
| *CFC*-Dokumentation | Dokumentation durch die Ausdrucke der *Safety Matrix* |

## Prinzipielle Arbeitsweise

### Analysephase

Bei der Risikoanalyse der Anlage kann der Anwender den im Verlauf eines Prozesses auftretenden Ereignissen (Causes) exakt definierte Reaktionen (Effects) zuordnen und damit das Systemverhalten der Anlage festlegen.

In der *Safety Matrix* gibt der Anwender mögliche Prozessereignisse (ein oder mehrere Eingänge) ein, konfiguriert deren Art und Anzahl, logische Verknüpfungen, eventuelle Verzögerungen und Verriegelungen sowie ggf. tolerierbare Abweichungen.

Anschließend definiert er die Reaktionen (ein oder mehrere Ausgänge) auf ein bestimmtes Ereignis.

Die Verknüpfung von Causes und Effects erfolgt durch einfaches Anklicken der Zelle in deren Schnittpunkt.

Beim Speichern der *Safety Matrix* erfolgt eine Prüfung der Projektierung auf Plausibilität.

Die *Safety Matrix* dokumentiert die sicherheitstechnischen Funktionsgruppen (SIF), und die Cause/Effect-Matrix selbst ist ein wichtiger Bestandteil der Spezifikation des Sicherheitsprogramms.

### Realisierungsphase

Die Spezifikation des Sicherheitsprogramms erfolgt durch Projektieren der Cause/Effect-Parameter in der *Safety Matrix*. Anhand dieser Vorgaben generiert die *Safety Matrix* automatisch die F-Systems-Programmlogik auf *CFC*-Basis mit F-Bausteinen aus der *Safety Matrix*-Bibliothek.

Die *Safety Matrix* bietet darüber hinaus eine Versions- und Änderungsverfolgung und Funktionen zum Vergleichen von Matrizen und zur Unterstützung bei der Abnahme der Anlage.

#### Betriebsphase

Das Engineering Tool der *Safety Matrix* und der auf der SIMATIC *PCS 7* Operator Station betreibbare Viewer ermöglichen die Bedienung und Beobachtung der Anlage auch im Sicherheitsbetrieb. Der Signalstatus wird dabei online in der Cause/Effect-Matrix dargestellt.

Der Operator kann Erstalarmmeldungen anzeigen und speichern sowie sicherheitsrelevante Ereignisse aufzeichnen lassen. Parameteränderungen werden ebenso unterstützt wie Bypass-, Rücksetzen- und Übersteuern-Funktionen.

Safety Lifecycle-Managementfunktionen für die Versionsverwaltung sowie für die Dokumentation der Bedienereingriffe und Programmänderungen ergänzen die Projektierungs-, Betriebs- und Servicefunktionen der *Safety Matrix*.

#### Erreichbare Sicherheitsanforderungen

Mit der *Safety Matrix* erfüllen Sie die folgenden Sicherheitsanforderungen:

- bis Sicherheits-Integritätslevel (Safety Integrity Level) SIL3 nach IEC 61508
- bis Kategorie 4 nach EN 954-1
- bis Performance Level (PL) e nach ISO 13849-1:2006 bzw. nach EN ISO 13849-1:2008

## 1.2 Die Optionspakete der Safety Matrix

### Optionspakete und Funktionsumfang

Die Safety Matrix besteht aus drei Produkten, die auch einzeln als drei Optionspakete bezogen werden können.

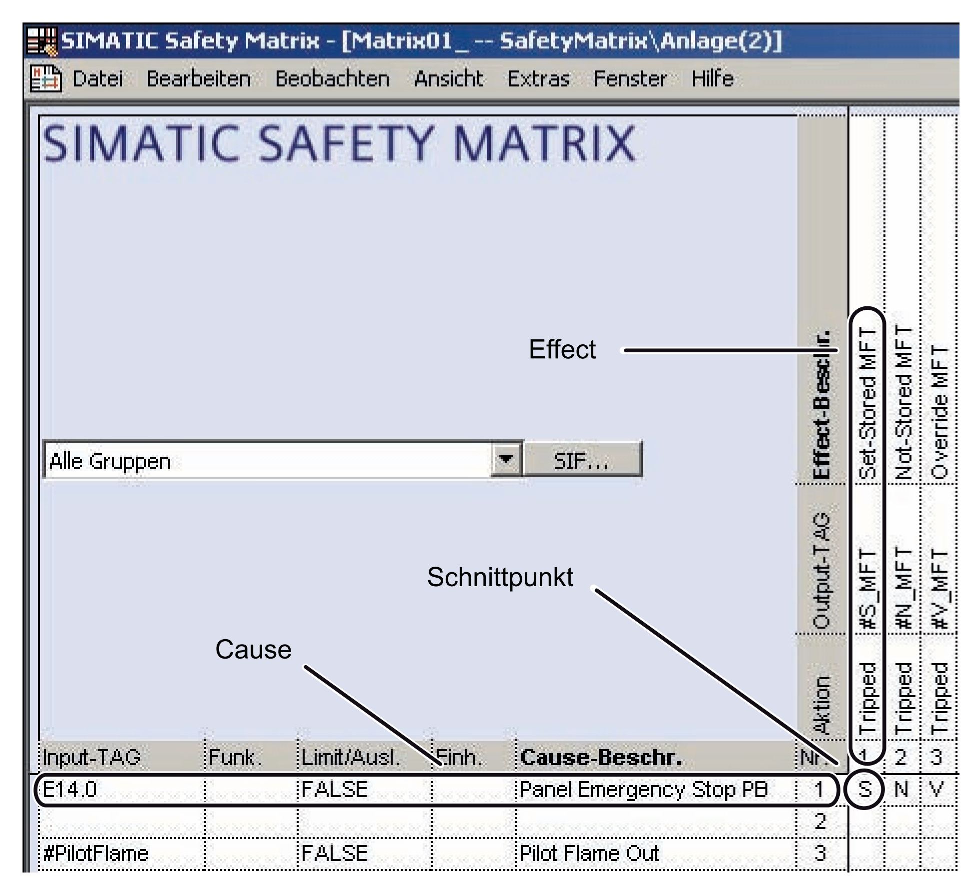
Tabelle 1- 1 Funktionsumfang der *Safety Matrix*-Optionspakete

| Optionspaket | Funktionsumfang | Umgebung | Betriebsart | Nutzungsphase |
|---|---|---|---|---|
| *Safety Matrix Editor* | Anlegen und Projektieren einer Safety Matrix auf einem PC außerhalb von *PCS 7* bzw. *STEP 7* inkl. Prüfung der Projektierung auf Plausibilität, Dokumentation und Erzeugung einer importierbaren .cem-Matrixdatei | Standalone | Offline | Analysephase (Planung und Projektierung) |
| *Safety Matrix Engineering Tool* | Anlegen (Importieren einer .cem-Matrixdatei), Projektieren einer Safety Matrix, automatische Generierung und Laden der *CFC*-Pläne inklusive Treiberbausteinen in ein *PCS 7*-Projekt, Bedienen und Beobachten mittels *STEP 7 SIMATIC Manager* auf einem *PCS 7*-Engineering System (ES) | Engineering System (ES) *PCS 7* bzw. *STEP 7* und *CFC* | Offline, Online | Analyse-, Realisierungs- und Betriebsphase (gesamter Safety Lifecycle) |
| *Safety Matrix Viewer* | Bedienen und Beobachten mittels Bildbaustein auf einer *PCS 7*-Operator Station (OS) | *PCS 7*-Operator Station (OS) | Online | Betriebsphase (Bedienen und Beobachten) |

# 1.3 Beispielansicht einer Safety Matrix

## Beispielansicht einer Safety Matrix

Das folgende Bild zeigt die Beispielansicht einer Safety Matrix.




Beispiel: Wird der Cause 1 aktiv (Auslösen bei FALSE, also bei Input-TAG = "0"), wird der Effect 1 ausgelöst und gespeichert.

# 1.4 Begriffsbestimmungen

Im Folgenden werden zentrale Begriffe der Safety Matrix erläutert.

## Cause

Ein Cause ( = Ursache) repräsentiert ein Prozessereignis.

Der Cause bildet die Ursache für die Aktivierung eines Effect. Es müssen bestimmte Bedingungen erfüllt sein, damit der Cause aktiv wird und somit über einen Schnittpunkt auf einen Effect wirkt.

Als Input-Typ stehen analoge oder diskrete Werte zur Auswahl. Die Werte von mindestens einem und maximal drei Input-TAGs bilden zusammen über den Funktionstyp einen Cause.

Sie können maximal 128 Causes anlegen.

Causes sind in der Safety Matrix in den Zeilen angeordnet.

## Effect

Ein Effect ( = Wirkung) repräsentiert die Reaktion der Safety Matrix, die sie auf den Prozess ausübt.

Es müssen bestimmte Bedingungen erfüllt sein, damit der Effect aktiv wird und somit über seine Output-TAGs auf den Prozess wirkt.

Die Werte von mindestens einem und maximal vier diskreten Output-TAGs bilden die Wirkung auf den Prozess. Die Aktivierung eines Effect hängt von verschiedenen Faktoren ab (Zustand der zugeordneten Causes, Typ des Schnittpunkts, eingestellte Optionen des Effect).

Sie können maximal 128 Effects anlegen.

Effects sind in der Safety Matrix in den Spalten angeordnet.

## Schnittpunkt

Die Safety Matrix-Schnittpunkte legen fest, welche Causes auf die jeweiligen Effects wirken.

Sie können bis zu 1024 Schnittpunkte definieren.

## Aktiv

Ein Cause oder Effect kann aktiv werden, was bedeutet, dass er ausgelöst wurde.

Ob und wann ein Cause aktiv wird, wird durch die Input-TAGs, den Funktionstyp und die Optionen des Cause bestimmt.

Die Aktivierung eines Effect hängt von der Beziehung (über die Schnittpunkte) zu den Causes und den Optionen des Effect ab. Ist ein Effect aktiv, so werden die Output-TAGs auf "0" bzw. "1" gesetzt, je nach Option für "Energize-to-trip".

## Inaktiv

Ein Cause oder Effect kann inaktiv werden, was bedeutet, die Bedingungen für die Aktivierung sind nicht erfüllt.

Ob der Cause inaktiv wird, wird durch die Input-TAGs, den Funktionstyp und die Optionen des Cause bestimmt.

Die Deaktivierung eines Effect hängt von der Beziehung (über die Schnittpunkte) zu den Causes und den Optionen des Effect ab. Ist ein Effect inaktiv, so werden die Output-TAGs auf "0" bzw. "1" gesetzt, je nach Option für "Energize-to-trip".

## Energize-to-trip (ETT)

Auslösen bei TRUE: Der Cause ist aktiv, wenn Input-TAG = "1" (high-active). Der Output-TAG ist "1", wenn der Effect aktiv ist.




**Sicherer Zustand bei digitaler F-Peripherie**

Grundlage des Sicherheitskonzeptes ist es, dass für alle Prozessgrößen ein sicherer Zustand existiert. Bei digitaler F-Peripherie ist das der Wert "0", dies gilt für Geber wie für Aktoren. Deshalb müssen Sie in der Applikation geeignete Maßnahmen, z. B. Redundanzen, realisieren.

## Deenergize-to-trip (DTT)

Auslösen bei FALSE: Der Cause ist aktiv, wenn Input-TAG = "0" (low-active). Der Output-TAG ist "0", wenn der Effect aktiv ist. Diese negative Logik ist die Standardeinstellung für die Eingänge und Ausgänge der Safety Matrix.

Standardmäßig bewirkt der Input-TAG nach dem "Deenergize-to-trip"–Prinzip eine Aktivierung des Cause, was bedeutet, dass ein Cause aktiv wird, wenn der Input-TAG "0" ist. Der Cause wird inaktiv, wenn der Input-TAG "1" ist. Hat ein Cause mehrere Input-TAGs, so ist der Funktionstyp für eine Aktivierung des Cause noch zu berücksichtigen.

Mit den Output-TAGs verhält es sich ebenso. Ist der Effect aktiv, so werden die Output-TAGs auf "0" gesetzt, ist er inaktiv, auf "1".

## Funktionstyp

Bestimmt gemeinsam mit den Input-TAGs und deren Optionen, ob und wann ein Cause aktiv oder inaktiv wird.

- Normal: ein Input-TAG
- 2oo3: drei Input-TAGs, 2 von 3 Auslösekriterien müssen erfüllt sein
- UND: 2-3 Input-TAGs, alle Auslösekriterien müssen erfüllt sein
- ODER: 2-3 Input-TAGs, mindestens ein Auslösekriterium muss erfüllt sein
- Nur Kommentar

## Bypass

Umgehungsfunktion, die in der Regel für Wartungszwecke verwendet wird (z. B. zum Überprüfen einer Effect-Logik, Austausch eines Sensors).

Als "Bypass-TAG" kann ein boolescher TAG ausgewählt bzw. eingegeben werden. Der Bypass wird aktiv, wenn der Wert des Bypass-TAG TRUE ist.

Neben dem "Bypass-TAG" kann auch der "Soft-Bypass" erlaubt werden. Dann kann der Bediener den Bypass manuell durch eine Bedienung über Secure Write setzen.

Bei aktivem Bypass kann ein Cause oder Effect nicht aktiv werden, obwohl er aufgrund seiner Auslösebedingung und Optionen aktiv sein sollte.

## Sicherheitstechnische Funktionsgruppen (SIF)

Sicherheitstechnische Funktionsgruppen (Safety Instrumented Function groups) können Sie nach Maßgabe Ihrer Anwendung selbst anlegen, d. h. Sie unterteilen Ihre Anwendung in Funktionsgruppen, die Sie dann im *Safety Matrix Engineering Tool* und *Safety Matrix Viewer* gezielt beobachten und ändern können (z. B. "Füllstandsmessung und Abschaltung").

Um diese Funktion nutzen zu können, müssen Sie die einzelnen Causes und Effects des Sicherheitsprogramms Ihren Sicherheitstechnischen Funktionsgruppen zuordnen. Dann können Sie einzelne, mehrere oder alle Sicherheitstechnischen Funktionsgruppen anzeigen.

## Secure Write

Durch die Funktionalität "Secure Write" werden Bedienungen an der Safety Matrix vorgenommen. Dies kann im Online-Betrieb des *Safety Matrix Engineering Tools* bzw. von der PCS 7 OS über den *Safety Matrix Viewer* erfolgen.

## Transaktion für Secure Write

Eine Transaktion zur Bedienung einer Safety Matrix über Secure Write führen Sie im Online-Betrieb des *Safety Matrix Engineering Tools* bzw. von der PCS 7 OS über den *Safety Matrix Viewer* durch. Die Transaktion besteht aus einer Bedienfolge, die von einem oder zwei Bedienern durchgeführt werden kann.

Die Transaktion muss innerhalb eines vom Anwender festzulegenden Zeitintervalls abgeschlossen sein (Timeout). Wenn die Transaktion nicht beendet wird, bevor der Timeout abgelaufen ist, wird die Transaktion automatisch abgebrochen.

# 1.5 Wegweiser zur Vorgehensweise

Dieses Kapitel gibt Ihnen einen Kurzüberblick über die Vorgehensweise beim Einsatz der Safety Matrix Komponenten innerhalb des *PCS 7*-Automatisierungssystems.

## Wegweiser zur Vorgehensweise

Tabelle 1- 2 Wegweiser zur Vorgehensweise

| Schritt | Was ist zu tun? | Safety Matrix-Komponente | Siehe Kapitel |
|---|---|---|---|
| 1 | Einfügen einer neuen Safety Matrix | Engineering Tool | 3.1 |
| 2 | Bearbeiten der Eigenschaften der Safety Matrix | Engineering Tool, Editor | 4.2 |
| 3 | Projektieren der Funktionen der Safety Matrix:<br>Causes<br>Effects<br>Schnittpunkte | Engineering Tool, Editor | 4<br>4.3<br>4.4<br>4.5 |
| 4 | Safety Matrix transferieren | Engineering Tool | 6 |
| 5 | Übersetzen und Laden | Engineering Tool | 7 |
| 6 | Bedienen und Beobachten | Engineering Tool, Viewer | 8 |
| 7 | Dokumentation einer Safety Matrix | Engineering Tool, Editor | 9 |
| 8 | Abnahme einer Safety Matrix | Engineering Tool | 10 |

# Installieren 2

## 2.1 Voraussetzungen für die Installation

### Hardware-Komponenten

Zu den Hardware-Komponenten von S7 F/FH Systems siehe das Programmier- und Bedienhandbuch "S7 F/FH Systems, Projektieren und Programmieren (http://support.automation.siemens.com/WW/view/de/2201072)".

### Software-Voraussetzungen

Für den Betrieb der Safety Matrix-Komponenten mit ihrem gesamten Funktionsumfang ist die folgende Software erforderlich.




**Betrieb der Safety Matrix**

Die Safety Matrix-Komponenten dürfen Sie nur in den freigegebenen Systemumgebungen betreiben.

Ausdrücklich nicht erlaubt ist der Betrieb auf Terminal-Server/Clients oder auf einem virtuellen Server/System.

### Safety Matrix Engineering Tool

Damit Sie das *Safety Matrix Engineering Tool* V6.2 betreiben können, müssen Sie folgende Softwarepakete auf dem ES installiert haben:

- Unterstützte Betriebssysteme
  - Windows XP SP2 oder SP3
  - Windows 2003 Server SP1 oder SP2, jeweils inkl. R2
- Erforderliche Optionspakete
  - *S7 F Systems* ab V5.2 SP1
  - F-Bibliothek *Failsafe Blocks* (V1_2) bzw. *S7 F Systems Lib* V1_3
  - Zum Offline-Testen: *S7-PLCSIM*, abhängig von der installierten *S7 F Systems*-Version
  - Automation License Manager (ALM) ab V3.0 SP1
- Bei Einsatz mit *PCS 7*:
  - *PCS 7* V6.1 SP3 bzw. *PCS 7* V7.0 ab SP3 bzw. *PCS 7* V7.1 ab HF1
  - Windows-Version entsprechend *PCS 7*-Version
- Bei Einsatz ohne *PCS 7*:
  - *STEP 7* ab V5.4 SP3
  - *CFC* ab V7.0 SP1

### Safety Matrix Viewer

Damit Sie den *Safety Matrix Viewer* V6.2 betreiben können, müssen Sie folgende Softwarepakete auf der OS installiert haben:

- Unterstützte Betriebssysteme
  - Windows XP SP2 oder SP3
  - Windows 2003 Server SP1 oder SP2 RC2
- *PCS 7* V6.1 SP3 bzw. *PCS 7* V7.0 ab SP3 bzw. *PCS 7* V7.1 ab HF1
- Automation License Manager (ALM) ab V3.0 SP1

Mit dem *Safety Matrix Viewer* V6.2 können Sie Matrizen der Versionen V5.2, V6.1 und V6.2 bedienen und beobachten.

### Safety Matrix Editor

Damit Sie den *Safety Matrix Editor* V6.2 betreiben können, müssen Sie folgende Softwarepakete auf Ihrem PC installiert haben:

- Windows XP ab SP2 bzw. Windows Server 2003 ab SP 1

## 2.2 Installieren

---

**Hinweis**

Installationen von Vorgängerversionen der Safety Matrix-Komponenten müssen vor der Installation der *Safety Matrix* V6.2 deinstalliert werden.

---

**Hinweis**

Für die Installation des *Safety Matrix Engineering Tool/Viewer* V6.2 gelten die gleichen Voraussetzungen, wie im *PCS 7*-Bedienhandbuch "PC-Konfiguration und Autorisierung (http://support.automation.siemens.com/WW/view/de/27002558)" beschrieben.

---



**Installierte Version der Safety Matrix-Komponenten prüfen**

Nach der Installation der Safety Matrix-Komponenten ist die jeweilige Version über "Installierte SIMATIC Software" (VersionView) zu prüfen.

## Liesmich-Dateien lesen

Wichtige aktuelle Informationen über die gelieferte Software finden Sie in den Liesmich-Dateien "*Safety Matrix Engineering Tool* V6.2 – Liesmich", "*Safety Matrix Viewer* V6.2 – Liesmich", "*Safety Matrix Editor* V6.2 – Liesmich" sowie "Safety Matrix AS-OS-Engineering – Liesmich". Diese Dateien können Sie sich am Ende des jeweiligen Setup-Programms anzeigen lassen. Zu einem späteren Zeitpunkt können Sie die Liesmich-Datei mit dem Befehl **Start > SIMATIC > Produkt-Hinweise > Deutsch** öffnen. Sie finden die Liesmich-Dateien im Installationsverzeichnis der jeweiligen Safety Matrix-Komponente.

## Safety Matrix Engineering Tool V6.2 installieren

1. Starten Sie Ihre ES. Stellen Sie sicher, dass keine Applikationen von *STEP 7* geöffnet sind.
2. Legen Sie die Produkt-CD des *Safety Matrix Engineering Tool* V6.2 ein.
3. Rufen Sie das Programm SETUP.EXE auf der CD auf.
4. Folgen Sie den Anweisungen des Setup-Programms.
5. Wenn Sie Safety Matrizen in einer *PCS 7*-Umgebung einsetzen, aktivieren Sie das Kontrollkästchen für "AS-OS-Engineering".

## Safety Matrix Viewer V6.2 installieren

1. Starten Sie Ihre ES/OS. Stellen Sie sicher, dass keine SIMATIC-Applikationen geöffnet sind.
2. Legen Sie die Produkt-CD des *Safety Matrix Viewer* V6.2 ein.
3. Rufen Sie das Programm SETUP.EXE auf der CD auf.
4. Folgen Sie den Anweisungen des Setup-Programms.

## Safety Matrix Editor V6.2 installieren

1. Starten Sie Ihren PC.
2. Legen Sie die Produkt-CD des *Safety Matrix Editor* V6.2 ein.
3. Rufen Sie das Programm SETUP.EXE auf der CD auf.
4. Folgen Sie den Anweisungen des Setup-Programms.

## License Key (Nutzungsberechtigung)

Für die Komponenten der *Safety Matrix* V6.2 ist jeweils ein License Key erforderlich. Der License Key wird wie bei *STEP 7* und den Optionspaketen installiert. Informationen zur Installation und Handhabung der License Keys finden Sie in der Liesmich-Datei und in der Basishilfe von *STEP 7*.

## Dokumentation

Wenn eine der Komponenten der *Safety Matrix* V6.2 installiert wird, dann wird für Deutsch und Englisch ein Shortcut mit dem Namen ‚Safety Matrix - Engineering Tool' im jeweiligen SIMATIC-Verzeichnis für Handbücher abgelegt (**Start > SIMATIC > Dokumentation**).

## 2.3 Deinstallieren der Safety Matrix V6.2-Komponenten

### Safety Matrix V6.2-Komponenten deinstallieren

**Hinweis**

Für die Deinstallation des *Safety Matrix Engineering Tool/Viewer* V6.2 gelten die gleichen Voraussetzungen, wie im Handbuch "PCS 7 V7.0 PC-Konfiguration und Autorisierung (http://support.automation.siemens.com/WW/view/de/27002558)" beschrieben.

Benutzen Sie das unter Windows übliche Verfahren zur Deinstallation:

1. Starten Sie unter Windows den Dialog zur Installation von Software durch Doppelklick auf das Symbol "Software" in der "Systemsteuerung".
2. Markieren Sie jeweils den Eintrag "SIMATIC SafetyMatrix Engineering Tool V6.2", "SIMATIC SafetyMatrix AS/OS Engineering V6.2" und/oder "SIMATIC SafetyMatrix Viewer V6.2" oder "SIMATIC SafetyMatrix Editor V6.2" in der Liste der installierten Software. Klicken Sie auf die Schaltfläche "Hinzufügen/Entfernen", um die Software zu deinstallieren.

## 2.4 Einbringen des neuen Safety Matrix-Bausteinsymbols in die PCS 7 OS

**Hinweis**

Der *Safety Matrix Viewer* V6.2 beinhaltet Bausteinsymbole für die *Safety Matrix* V6.2 und ein Bausteinsymbol für die *Safety Matrix* V5.2 oder V6.1. Somit können auf einer OS folgende *Safety Matrix*-Versionen gemeinsam betrieben werden:

- V6.2 und V5.2
- V6.2 und V6.1

### Bilder konvertieren

Wenn Sie eine *PCS7*-Version ab V7.0 verwenden, müssen Sie die Bilder noch auf Ihre verwendete *WinCC*-Version konvertieren. Führen Sie dazu die folgenden Schritte aus.

1. Starten Sie den **WinCC-Explorer** für die im Safety Matrix-Projekt enthaltene OS.
2. Klicken Sie mit der rechten Maustaste auf den Eintrag "Graphics Designer" im **WinCC-Explorer**.
3. Wählen Sie "Konvertieren der Bilder" im Kontextmenu. Es werden alle Bilder konvertiert.
4. Wählen Sie für einen erneuten Einsatz des **OS-Projekteditors** die folgenden Bilder im Register "Grunddaten" ab:
   - @PG_F_MATCTL*
   - @PG_F_MA_AL*
   - @PG_F_SC_AL*
   - @PG_F_SE_AL*
   - @PCS7Typicals_S7FSMTX.PDL

### Einbringen in ein vorhandenes Safety Matrix-Projekt

Um die neuen Funktionen des Safety Matrix-Bildbausteins in einem bereits vorhandenen Projekt nutzen zu können, müssen Sie das Projekt aktualisieren.

1. Starten Sie dazu den **WinCC-Explorer** für die im Safety Matrix-Projekt enthaltene OS.
2. Öffnen Sie den **OS-Projekteditor** und klicken Sie auf **OK**. Das Projekt wird neu konfiguriert und damit das neue Bausteinsymbol übernommen.
3. Öffnen Sie den **Global Script C-Editor** und wählen Sie den Menübefehl **Optionen > Header neu generieren** an.

### Ohne Aktualisierung der *Safety Matrix*-Bibliothek

Falls Sie sich für den Einsatz der Safety Matrix ohne Aktualisierung der *Safety Matrix*-Bibliothek entschieden haben, führen Sie noch folgenden Schritt aus:

- Um das neue Bausteinsymbol auch in bereits vorhandene Anlagenbilder zu übernehmen, müssen Sie das jeweilige Projekt neu kompilieren.
  Projektieren Sie ggf. die gewünschten Berechtigungen an den Bausteinsymbolen.

### Mit Aktualisierung der *Safety Matrix*-Bibliothek

Falls Sie sich für den Einsatz der Safety Matrix mit Aktualisierung der *Safety Matrix*-Bibliothek entschieden haben, gehen Sie folgendermaßen vor:

- Um das neue Bausteinsymbol auch in bereits vorhandene Anlagenbilder zu übernehmen, müssen Sie das jeweilige Projekt neu kompilieren.
  Beachten Sie, dass die TH-Zuordnung und die Vergabe von Berechtigungen jetzt im *Safety Matrix Engineering Tool* stattfindet (siehe Kapitel "Der Dialog "Eigenschaften" der Safety Matrix (Seite 75)").

### Neukompilieren des betreffenden Projekts

1. Starten Sie dazu den *SIMATIC Manager*.
2. Stellen Sie sicher, dass in den Objekteigenschaften des betreffenden Bildobjektes im Register "Bausteinsymbole" die Option "Bausteinsymbole aus der Technologischen Hierarchie ableiten" aktiviert ist. (Dies ist bei *PCS 7* ab V7 voreingestellt.)

   ---

   **Hinweis**

   Sollen beim anschließenden OS Übersetzen eines bestehenden Bildes die vom Anwender vergebenen Einstellungen am Bausteinsymbol einer Safety Matrix beibehalten werden, so deaktivieren Sie für dieses *WinCC*-Bild die Option "Bausteinsymbole aus der Technologischen Hierarchie ableiten".

   ---

3. Markieren Sie das OS-Objekt und wählen Sie aus dem Kontextmenü "Übersetzen", um die OS zu übersetzen.

   Für *PCS 7* < V7: Stellen Sie sicher, dass im Assistent "OS Übersetzen" beim Wählen der Übersetzungsdaten und des Übersetzungsumfangs die Option "Bausteinsymbole erzeugen/aktualisieren" aktiviert ist. (Dies erfolgt bei *PCS 7* ab V7 automatisch.)
4. Betätigen Sie im letzten Dialog des Assistenten "OS Übersetzen" die Schaltfläche "Übersetzen".

### Ergebnis

Nachdem Sie diese Schritte durchgeführt haben, enthält Ihr Projekt das neue Safety Matrix-Bausteinsymbol.

Wiederholen Sie diese Schritte für alle Projekte.

# 2.5 Hochrüsten auf Safety Matrix V6.2

## 2.5.1 Übersicht zum Hochrüsten

### Prinzipielle Vorgehensweise zum Hochrüsten

Beim Hochrüsten der *Safety Matrix* V5.2 bzw. V6.1 auf V6.2 sind folgende Schritte zwingend in dieser Reihenfolge einzuhalten:

1. Hochrüsten der Safety Matrix, wie im Folgenden beschrieben.
2. Ggf. F-Bibliothek *S7 F Systems Lib* hochrüsten, wie beschrieben im Programmier- und Bedienhandbuch "S7 F/FH Systems, Projektieren und Programmieren (http://support.automation.siemens.com/WW/view/de/2201072) ".
3. Ggf. *PCS 7* hochrüsten, wie in der *PCS 7*-Dokumentation beschrieben.

### Anwenderszenarien zum Hochrüsten

| Umstieg von… | Aktualisierung der *Safety Matrix*-Bibliothek | ...auf *Safety Matrix* V6.2 |
|---|---|---|
| *Safety Matrix* V5.2 | Erforderlich | Anwenderszenario 1 (Seite 31) |
| *Safety Matrix* V6.1 | Ja | Anwenderszenario 2 (Seite 36) |
| *Safety Matrix* V6.1 | Nein | Anwenderszenario 3 (Seite 40) |
| *Safety Matrix* V5.2/V6.1, nur Hochrüsten des *Safety Matrix Viewer* | Nein | Anwenderszenario 4 (Seite 42) |

## Allgemeine Hinweise zum Hochrüsten

Nach Installation der *Safety Matrix* V6.2 bedingen Änderungen an bestehenden Safety Matrizen ein Hochrüsten. Dieses Hochrüsten kann mit oder ohne Aktualisierung der *Safety Matrix*-Bibliothek erfolgen, siehe obige Tabelle.

Erfolgt eine Hochrüstung mit Aktualisierung der *Safety Matrix*-Bibliothek, so erfordert dies einen STOP der F-CPU.

### Varianten beim Hochrüsten

Bevor Sie ein bestimmtes Projekt auf *Safety Matrix* V6.2 hochrüsten, müssen Sie sich für eine der beiden Varianten entscheiden:

| Variante | Konsequenzen | |
|---|---|---|
| | Vorteile | Nachteile |
| Ohne Aktualisierung der *Safety Matrix*-Bibliothek | • Gleich bleibendes Sicherheitsprogramm, damit kein CPU-STOP erforderlich | • Neue Funktionen sind nur eingeschränkt nutzbar |
| Mit Aktualisierung der *Safety Matrix*-Bibliothek | • Erweitertes Engineering<br>• Erweiterte Funktionalität für Bedienen und Beobachten<br>• Versionsmix auf der OS möglich | • Geändertes Sicherheitsprogramm, damit CPU-STOP erforderlich |

Wenn Sie die Safety Matrix mit Aktualisierung der *Safety Matrix*-Bibliothek hochrüsten, können Sie den vollen Funktionsumfang des verbesserten Alarmverhaltens nutzen. Beachten Sie dazu die Kapitel zur "Meldungsprojektierung (Seite 61)" und Kapitel "Der Dialog "Eigenschaften" der Safety Matrix (Seite 75)", Register 'Alarme'. Die Meldungsprojektierung für einzelne Causes/Effects ist in der Voreinstellung deaktiviert.

### 2.5.2 Anwenderszenario 1

#### Ziel

Aktualisierung des *Safety Matrix Engineering Tools* sowie der *Safety Matrix*-Bibliothek.

#### Einleitung

Dieses Anwenderszenario hilft Ihnen beim Umstieg von *Safety Matrix* V5.2 auf *Safety Matrix* V6.2.

#### Voraussetzung

Voraussetzung ist ein übersetztes und geladenes Projekt (ggf. abgenommen). In diesem Projekt müssen die Bausteine der F-Bibliothek *Failsafe Blocks* (V1_2 + SP1) oder höher enthalten sein. Sie können dies wie folgt überprüfen:

- Öffnen Sie im *SIMATIC Manager* den Bausteinordner des Programms in der Detailansicht. In der Spalte "Version (Header)" muss für die nachfolgenden F-Kanaltreiber die Angabe "3.1" (oder höher) stehen:
  - F_CH_DI
  - F_CH_DO
  - F_CH_AI

Es dürfen offline keine Änderungen vorhanden sein, die nicht auch online geladen sind.

#### Konsequenzen

- Änderung der Gesamtsignatur
- Gesamtladen mit CPU-STOP erforderlich

## Vorgehensweise

1. Legen Sie vor der Installation der *Safety Matrix* V6.2 für den späteren Vergleich eine Sicherungskopie des gesamten S7-Projektes an.
2. Installieren Sie *Safety Matrix* V6.2 auf der ES.
3. Installieren Sie ggf. das *Safety MatrixAS-OS-Engineering* auf der ES.
4. Installieren Sie ggf. *Safety Matrix Viewer* auf der ES/OS.
5. Klicken Sie im S7-Programmordner mit der rechten Maustaste auf den Ordner "Matrizen" und wählen Sie die **Objekteigenschaften** des Matrixordners.
6. Wählen Sie im Register "Matrix" der Objekteigenschaften die für dieses S7-Programm zu verwendende Safety Matrix-Bibliothek "SafetyMatrix Lib (V1_3)" aus.
7. Bestätigen Sie die folgenden Abfragen. Die Bausteine werden in den S7-Programmordner kopiert.
8. Öffnen Sie die Safety Matrix und transferieren Sie sie mit folgenden Einstellungen der Transfer-Optionen:
   – Transfer-Option "Importierte Kanaltreiber verwenden (IEA Unterstützung)" deaktiviert
   – Transfer-Option "Plan + Parameter" aktiviert
   – Transfer-Option "Hierarchische Plan-Anschlüsse bereinigen" aktiviert
   – Transfer-Option "Bausteine platzieren" aktiviert mit Option "Alle aktualisieren"
9. Führen Sie Schritt 8. für alle vorhandenen Safety Matrizen durch. Währenddessen sind keine weiteren *CFC*-Aktionen erlaubt.
10. Übersetzen Sie das SIMATIC-Projekt.
11. Vergleichen Sie mithilfe des Menübefehls **Extras > Vergleiche Programme** im *Safety Matrix Engineering Tool* das Sicherheitsprogramm mit der Sicherungskopie aus Schritt 1.

    Für jede Safety Matrix wird nach erfolgreichem Hochrüsten folgende Änderung aufgelistet:

    ```
    Matrix unkritisch geändert, Neue Version der Matrix, SWC-Parameter
    geändert
    ```
12. Vergleichen Sie zusätzlich das Sicherheitsprogramm mit der Sicherungskopie. Verwenden Sie dazu im *SIMATIC Manager* im Dialog "Sicherheitsprogramm bearbeiten" die Schaltfläche **Vergleichen...**.

## Ergebnis des Vergleichs in Schritt 12

Das Ergebnis des Vergleichs ist eine Auflistung mit drei Abschnitten: "Ablaufebene", "Plan" und "geänderte Systempläne". Aufgelistete Änderungen der Matrix im Abschnitt "Plan" (Format: `Plan "Matrixname", Plan "@Matrixname"...`) sind mit dem Menübefehl **Extras > Vergleiche Programme** besser interpretierbar und können daher an dieser Stelle ignoriert werden. Der Plan "@FMatrices" wird automatisch erstellt.

Im Abschnitt "Ablaufebene" werden nach erfolgreichem Hochrüsten folgende Änderungen aufgelistet:

In jedem OB mit Sicherheitsprogramm:

```
Baustein "@F_CycCo-OBxx\F_TEST": Signatur geändert
```

In jeder Ablaufgruppe mit Safety Matrix-F-Bausteinen:

- ein Eintrag je Safety Matrix:

```
Baustein "MatrixName\@MatrixName\Libvers(F_AND4)": ergänzt
```

- je Safety Matrix ein Abschnitt (**Status_DB**):

```
Baustein "Matrixname\@Matrixname\C_Status(F_StatDB)": Signatur
geändert, Schnittstelle geändert 'xxx'<->'xxx'
SM_VER Wert: ’16#0003’ <- ’16#0001’
DB_Num Struktur: 'CHAR' <- 'BOOL'
FlowCnt gelöscht
CYC gelöscht

Baustein "Matrixname\@Matrixname\E_Status(F_StatDB)": Signatur
geändert, Schnittstelle geändert 'xxx'<->'xxx'
SM_VER Wert: '16#0003' <- '16#0001'
DB_Num Struktur: 'CHAR' <- 'BOOL'
FlowCnt gelöscht
CYC gelöscht
```

- je Safety Matrix ein Abschnitt für jeden **F_Cause F-FB**

```
Baustein "Matrixname\@Matrixname\Cxx(F_Cause)": Signatur geändert,
Schnittstelle geändert 'xxx'<->'xxx'
SM_VER Wert: '16#0003' <- '16#0001'
C_Status_DB Struktur: 'CHAR' <- 'BOOL'
DB_GROUP ergänzt
MatrixSize Wert: 'nicht verschaltet' <-
'verschaltet (Matrixname\@Matrixname\Matrixname\Size)'
```

Für jeden verwendeten diskreten bzw. analogen TAG einer anderen Safety Matrix (Präfix"@"):

```
AnschlussName Wert: 'MatrixName1\MatrixName1\TAG-Name\Q' <-
'@MatrixName\TAG-Name'
```

bzw.

```
AnschlussName Wert: 'MatrixName1\MatrixName1\TAG-Name\V' <-
'@MatrixName\TAG-Name'
```

Folgende Standardparameter für das Bedienen und Beobachten bzw. Melden:

```
P_LIMV_xx ergänzt
VMODx_R_yy ergänzt
VMODx_B_yy ergänzt
HMI ergänzt
DB_NUM ergänzt
CYC gelöscht
```

- je Safety Matrix ein Abschnitt für den **F_Inters F-FB**

```
Baustein " Matrixname\@Matrixname\Inters(F_Inters)": Signatur
geändert, Schnittstelle geändert 'xxx'<->'xxx'
SM_VER Wert: '16#0003' <- '16#0001'
C_Status_DB Struktur: 'CHAR' <- 'BOOL'
MatrixSize Wert: 'nicht verschaltet' <-
'verschaltet (MatrixName\@MatrixName\MatrixName\Size)'
Inters_xxxx ergänzt
E_Trip_DB Struktur: 'CHAR' <- 'BOOL'
CYC gelöscht
```

Mit Hilfe des Menübefehls **Extras > Vergleiche Programme** sowie des Konfigurationsreports können Sie einen Nachweis über die nicht verwendeten Schnittstellen erstellen.

- je Safety Matrix ein Abschnitt für jeden **F_Effect F-FB**

```
Baustein "MatrixName\@MatrixName\Exx(F_Effect)": Signatur geändert,
Schnittstelle geändert 'xxx'<->'xxx'
SM_VER Wert: '16#0003' <- '16#0001'
E_Trip_DB Struktur: 'CHAR' <- 'BOOL'
E_Status_DB Struktur: 'CHAR' <- 'BOOL'
DB_GROUP ergänzt
MatrixSize Wert: 'nicht verschaltet' <-
'verschaltet (MatrixName\@MatrixName\MatrixName\Size)'
```

Folgende Standardparameter für das Bedienen und Beobachten bzw. Melden:

```
P_OVTM_xx ergänzt
DB_NUM ergänzt
CYC gelöscht
```

- je Safety Matrix ein Abschnitt für den **F_Matctl F-FB**

```
Baustein "MatrixName\@MatrixName\MatrixName(F_Matctl)": Signatur
geändert, Schnittstelle geändert 'xxx'<->'xxx'
SM_VER Wert: '16#0003' <- '16#0001'
C_Status_DB Struktur: 'CHAR' <- 'BOOL'
E_Trip_DB Struktur: 'CHAR' <- 'BOOL'
E_Status_DB Struktur: 'CHAR' <- 'BOOL'
MatrixID Wert: '16#xxxxxxxx' <- '16#xxxxxxxx'
TIME_SWC ergänzt
EN_SWC ergänzt
MatrixSig Wert: 'verschaltet (@MatrixName\MatrixSig)' <- 'nicht
verschaltet'
(ggf.)
Any_CB ergänzt
Any_EB ergänzt
Any_CW ergänzt
Any_EW ergänzt
CAct_Num ergänzt
EAct_Num ergänzt
DB_NUM ergänzt
IntEvent ergänzt
Size Wert: 'nicht verschaltet' <-
'verschaltet (MatrixName\@MatrixName\Exx\MatrixSize, …)'
ViewTime ergänzt
SWC_AKT ergänzt
SecCmdStat ergänzt
DurationMin ergänzt
Msec Wert: 'verschaltet (@MatrixName\Msec)' <- 'nicht verschaltet'
```

```
MaxMsec Wert: 'verschaltet (@MatrixName\MaxMsec)' <- 'nicht
verschaltet'
MtxVersion ergänzt
DB_NUM_D ergänzt
TempBuf1 Wert: '''' <- ''1234567890''
TempBuf Wert: '''' <- ''1234567890''
EV_ID gelöscht
ALARM_EN gelöscht
SecureDataVerf gelöscht
Dummy gelöscht
Dummy2 gelöscht
MSG_ERR gelöscht
MSG_STAT gelöscht
MSG_ACK gelöscht
DIAGSTAT gelöscht
```

Sollten Sie bei den Vergleichsergebnissen in den Schritten 11. oder 12. über die aufgelisteten Änderungen hinaus Einträge erhalten, so müssen Sie den anlagenspezifischen Hintergrund der Änderung ermitteln, bewerten und ggf. entsprechend Ihrer Anforderungen anpassen.

## Maßnahmen nach dem Hochrüsten

Nach dem erfolgreichen Hochrüsten der Safety Matrix sind die folgenden Maßnahmen durchzuführen.

1. Damit Sie die Safety Matrizen nach dem Hochrüsten bedienen können, müssen Sie die Eingangsparameter EN_SWC aller hierarchischen Pläne der Matrixlogik ("@MatrixName") verschalten, siehe Kapitel "Transaktion für Secure Write (Seite 136)".
2. Stellen Sie das Zeitintervall für eine Transaktion anlagenspezifisch ein, speziell dann, wenn Sie die Funktion "2-Bediener-Szenario" auf der *PCS 7* OS nutzen möchten. Diese Zeit kann im Dialog "Eigenschaften", Register "Parameter" frei konfiguriert werden, Standardeinstellung ist 60 s.
3. Nach dem erfolgreichen Hochrüsten kann eine Änderungsabnahme gemäß Kapitel "Abnahme einer Safety Matrix (Seite 159)" erfolgen. Für die unter den Schritten 11. und 12. aufgelisteten Änderungen ist kein weiterer Funktionstest erforderlich.
4. Rüsten Sie die Bausteinsymbole in den OS-Bildern hoch, wie beschrieben im Kapitel "Einbringen des neuen Safety Matrix-Bausteinsymbols in die PCS 7 OS (Seite 27)".
5. Übersetzen und laden Sie die OS.
6. Laden Sie das S7-Programm in die F-CPU.

### 2.5.3 Anwenderszenario 2

#### Ziel

Aktualisierung des *Safety Matrix Engineering Tools* sowie der *Safety Matrix*-Bibliothek.

#### Einleitung

Dieses Anwenderszenario hilft Ihnen beim Umstieg von *Safety Matrix* V6.1 auf *Safety Matrix* V6.2 mit Aktualisierung der *Safety Matrix*-Bibliothek.

#### Voraussetzung

Voraussetzung ist ein übersetztes und geladenes Projekt (ggf. abgenommen). In diesem Projekt müssen die Bausteine der F-Bibliothek *Failsafe Blocks* (V1_2 + SP1) oder höher enthalten sein. Sie können dies wie folgt überprüfen:

- Öffnen Sie im *SIMATIC Manager* den Bausteinordner des Programms in der Detailansicht. In der Spalte "Version (Header)" muss für die nachfolgenden F-Kanaltreiber die Angabe "3.1" (oder höher) stehen:
  - F_CH_DI
  - F_CH_DO
  - F_CH_AI

Es dürfen offline keine Änderungen vorhanden sein, die nicht auch online geladen sind.

#### Konsequenzen

- Änderung der Gesamtsignatur
- Gesamtladen mit CPU-STOP erforderlich

## Vorgehensweise

1. Legen Sie vor der Installation der *Safety Matrix* V6.2 für den späteren Vergleich eine Sicherungskopie des gesamten S7-Projektes an.
2. Installieren Sie *Safety Matrix* V6.2 auf der ES.
3. Installieren Sie ggf. das *Safety MatrixAS-OS-Engineering* auf der ES.
4. Installieren Sie ggf. *Safety Matrix Viewer* auf der ES/OS.
5. Klicken Sie im S7-Programmordner mit der rechten Maustaste auf den Ordner "Matrizen" und wählen Sie die **Objekteigenschaften** des Matrixordners.
6. Wählen Sie im Register "Matrix" der Objekteigenschaften die für dieses S7-Programm zu verwendende Safety Matrix-Bibliothek "SafetyMatrix Lib (V1_3)" aus.
7. Bestätigen Sie die folgenden Abfragen. Die Bausteine werden in den S7-Programmordner kopiert.
8. Öffnen Sie die Safety Matrix und transferieren Sie sie mit folgenden Einstellungen der Transfer-Optionen:
   – Transfer-Option "Importierte Kanaltreiber verwenden (IEA Unterstützung)" deaktiviert
   – Transfer-Option "Plan + Parameter" aktiviert
   – Transfer-Option "Hierarchische Plan-Anschlüsse bereinigen" aktiviert
   – Transfer-Option "Bausteine platzieren" aktiviert mit Option "Alle aktualisieren"
9. Führen Sie Schritt 8. für alle vorhandenen Safety Matrizen durch. Währenddessen sind keine weiteren *CFC*-Aktionen erlaubt.
10. Übersetzen Sie das SIMATIC-Projekt.
11. Vergleichen Sie mithilfe des Menübefehls **Extras > Vergleiche Programme** im *Safety Matrix Engineering Tool* das Sicherheitsprogramm mit der Sicherungskopie aus Schritt 1.

    Für jede Safety Matrix wird nach erfolgreichem Hochrüsten folgende Änderung aufgelistet:

    `Matrix unkritisch geändert, Neue Version der Matrix`

    Bei Einsatz der *S7 F Systems Lib* V1_3 erhalten Sie zusätzlich für jeden symbolisch verschalteten TAG eine unkritische Änderung in der Form:

    `VMODx_B/R_y: @Tagname <-> 0/0.0`
12. Vergleichen Sie zusätzlich das Sicherheitsprogramm mit der Sicherungskopie. Verwenden Sie dazu im *SIMATIC Manager* im Dialog "Sicherheitsprogramm bearbeiten" die Schaltfläche **Vergleichen...**.

## Ergebnis des Vergleichs in Schritt 12

Das Ergebnis des Vergleichs ist eine Auflistung mit drei Abschnitten: "Ablaufebene", "Plan" und "geänderte Systempläne". Aufgelistete Änderungen der Matrix im Abschnitt "Plan" (Format: `Plan "Matrixname"`, `Plan "@Matrixname"`...) sind mit dem Menübefehl **Extras > Vergleiche Programme** besser interpretierbar und können daher an dieser Stelle ignoriert werden. Der Plan "@FMatrices" wird automatisch erstellt.

### Ablaufebene

Im Abschnitt "Ablaufebene" werden nach erfolgreichem Hochrüsten folgende Änderungen aufgelistet:

**In jeder Ablaufgruppe mit Safety Matrix-F-Bausteinen:**

- je Safety Matrix ein Abschnitt (**Status_DB**):

```
Baustein " MatrixName\@MatrixName\C_Status(F_StatDB)": Signatur
geändert
SM_VER Wert: '16#0003' <- '16#0002'

Baustein " MatrixName\@MatrixName\E_Status(F_StatDB)": Signatur
geändert
SM_VER Wert: '16#0003' <- '16#0002'
```

- je Safety Matrix ein Abschnitt für jeden **F_Cause F-FB**

```
Baustein "Matrixname\@Matrixname\Cxx(F_Cause)": Signatur geändert,
Schnittstelle geändert 'xxx'<->'xxx'
SM_VER Wert: '16#0003' <- '16#0002'
DB_GROUP ergänzt
```

Folgende Standardparameter für das Bedienen und Beobachten bzw. Melden:

```
P_LIMV_xx ergänzt
VMODx_R_yy ergänzt
VMODx_B_yy ergänzt
DB_NUM ergänzt
Reserve gelöscht
```

- je Safety Matrix ein Abschnitt für den **F_Inters F-FB**

```
Baustein " Matrixname\@Matrixname\Inters(F_Inters)": Signatur
geändert, Schnittstelle geändert 'xxx'<->'xxx'
SM_VER Wert: '16#0003' <- '16#0002'
Inters_xxxx ergänzt
```

Mit Hilfe des Menübefehls **Extras > Vergleiche Programme** sowie des Konfigurationsreports können Sie einen Nachweis über die nicht verwendeten Schnittstellen erstellen.

- je Safety Matrix ein Abschnitt für jeden **F_Effect F-FB**

```
Baustein "MatrixName\@MatrixName\Exx(F_Effect)": Signatur geändert,
Schnittstelle geändert 'xxx'<->'xxx'
SM_VER Wert: '16#0003' <- '16#0002'
DB_GROUP ergänzt
```

Folgende Standardparameter für das Bedienen und Beobachten bzw. Melden:

```
P_OVTM_xx ergänzt
DB_NUM ergänzt
```

- je Safety Matrix ein Abschnitt für den **F_Matctl F-FB**

```
Baustein "MatrixName\@MatrixName\MatrixName(F_Matctl)": Signatur
geändert, Schnittstelle geändert 'xxx'<->'xxx'
SM_VER Wert: '16#0003' <- '16#0002'
Any_CB ergänzt
Any_EB ergänzt
Any_CW ergänzt
Any_EW ergänzt
CAct_Num ergänzt
EAct_Num ergänzt
DB_NUM ergänzt
IntEvent ergänzt
Size Wert: 'nicht verschaltet' <- 'verschaltet ()’
MtxVersion Wert: ''05.00'' <- ''04.00''
DB_NUM_D ergänzt
EV_ID gelöscht
```

### Geänderte Systempläne

Falls Sie die F-Bibliothek *Failsafe Blocks* (V1_2) verwenden, erhalten Sie zusätzlich im Abschnitt "geänderte Systempläne" folgende Anzeige

In jedem OB mit Sicherheitsprogramm:

```
Baustein "@F_CycCo-OBxx\F_TEST": Signatur geändert
```

Sollten Sie bei den Vergleichsergebnissen in den Schritten 11. oder 12. über die aufgelisteten Änderungen hinaus Einträge erhalten, so müssen Sie den anlagenspezifischen Hintergrund der Änderung ermitteln, bewerten und ggf. entsprechend Ihrer Anforderungen anpassen.

## Maßnahmen nach dem Hochrüsten

Nach dem erfolgreichen Hochrüsten der Safety Matrix sind die folgenden Maßnahmen durchzuführen.

1. Nach dem erfolgreichen Hochrüsten kann eine Änderungsabnahme gemäß Kapitel "Abnahme einer Safety Matrix (Seite 159)" erfolgen. Für die unter den Schritten 11. und 12. aufgelisteten Änderungen ist kein weiterer Funktionstest erforderlich.
2. Rüsten Sie die Bausteinsymbole in den OS-Bildern hoch, wie beschrieben im Kapitel "Einbringen des neuen Safety Matrix-Bausteinsymbols in die PCS 7 OS (Seite 27)".
3. Übersetzen und laden Sie die OS.
4. Laden Sie das S7-Programm in die F-CPU.

### 2.5.4 Anwenderszenario 3

#### Ziel

Aktualisierung des *Safety Matrix Engineering Tools*

#### Einleitung

Dieses Anwenderszenario hilft Ihnen beim Umstieg von *Safety Matrix* V6.1 auf *Safety Matrix* V6.2 ohne Aktualisierung der *Safety Matrix*-Bibliothek.

#### Voraussetzung

Voraussetzung ist ein übersetztes und geladenes Projekt (ggf. abgenommen). In diesem Projekt müssen die Bausteine der F-Bibliothek *Failsafe Blocks* (V1_2 + SP1) oder höher enthalten sein. Sie können dies wie folgt überprüfen:

- Öffnen Sie im *SIMATIC Manager* den Bausteinordner des Programms in der Detailansicht. In der Spalte "Version (Header)" muss für die nachfolgenden F-Kanaltreiber die Angabe "3.1" (oder höher) stehen:
  - F_CH_DI
  - F_CH_DO
  - F_CH_AI

Es dürfen offline keine Änderungen vorhanden sein, die nicht auch online geladen sind.

## Konsequenzen

- Keine Änderung des Sicherheitsprogramms
- Keine Änderung der Gesamtsignatur

---

**Hinweis**

Wenn Sie dieses Szenario wählen, verwendet die Safety Matrix weiterhin die Bausteine der Version V6.1, und es ist kein CPU-STOP erforderlich. Die Software-Oberfläche entspricht der Version V6.2, der Funktionsumfang allerdings entspricht weiterhin der Version V6.1, mit Ausnahme der folgenden Funktionen, die Ihnen jetzt zur Verfügung stehen:

- Sie können neben dem Zustand eines Cause oder Effect auch den Zustand eines Effect-TAG innerhalb der Safety Matrix an einem Input-TAG weiterverarbeiten ("Effect[x](TAG)[y]"). Siehe Kapitel "Dialog "Cause-Details" - Register "Konfigurieren" (Seite 87)".
- Sie können zusätzliche Farben für die Statusanzeigen der Causes, Effects und Schnittpunkte verwenden und frei zuordnen (siehe Kapitel "Die Dialoge "Anpassen" (Seite 80)").

Sie können zu einem beliebigen Zeitpunkt im Register "Matrix" der **Objekteigenschaften** des Matrixordners auf die Verwendung der "SafetyMatrix Lib (V1_3)" umstellen. Beachten Sie, dass diese Umstellung einen **CPU-STOP** bedingt (siehe Kapitel "Anwenderszenario 2 (Seite 36)").

Ein Rückwechseln von der "SafetyMatrix Lib (V1_3)" zur "SafetyMatrix Lib (V1_2)" ist nicht möglich.

---

## Vorgehensweise

1. Legen Sie vor der Installation der *Safety Matrix* V6.2 für den späteren Vergleich eine Sicherungskopie des gesamten S7-Projektes an.
2. Installieren Sie *Safety Matrix* V6.2 auf der ES.
3. Installieren Sie ggf. das *Safety MatrixAS-OS-Engineering* auf der ES.
4. Installieren Sie ggf. *Safety Matrix Viewer* auf der ES/OS.
5. Öffnen Sie die Safety Matrix und transferieren Sie sie mit den Einstellungen der Transfer-Optionen, welche Sie für die letzte Bearbeitung verwendet haben. Akzeptieren Sie die unkritischen Änderungen.
6. Führen Sie Schritt 5. für alle vorhandenen Safety Matrizen durch. Währenddessen sind keine weiteren *CFC*-Aktionen erlaubt.
7. Übersetzen Sie das SIMATIC-Projekt.
8. Vergleichen Sie mithilfe des Menübefehls **Extras > Vergleiche Programme** im *Safety Matrix Engineering Tool* das Sicherheitsprogramm mit der Sicherungskopie aus Schritt 1.

   Für jede Safety Matrix wird nach erfolgreichem Hochrüsten folgende Änderung aufgelistet:

   `Keine Unterschiede gefunden`

1. Vergleichen Sie zusätzlich das Sicherheitsprogramm mit der Sicherungskopie. Verwenden Sie dazu im *SIMATIC Manager* im Dialog "Sicherheitsprogramm bearbeiten" die Schaltfläche **Vergleichen...**.

#### Ergebnis des Vergleichs in Schritt 9

Keine Änderung des Sicherheitsprogramms.

#### Maßnahmen nach dem Hochrüsten

Nach dem erfolgreichen Hochrüsten der Safety Matrix sind die folgenden Maßnahmen durchzuführen.

1. Rüsten Sie die Bausteinsymbole in den OS-Bildern hoch, wie beschrieben im Kapitel "Einbringen des neuen Safety Matrix-Bausteinsymbols in die PCS 7 OS (Seite 27)".
2. Übersetzen und laden Sie die OS.

### 2.5.5 Anwenderszenario 4

#### Ziel

Aktualisierung des *Safety Matrix Viewer*

#### Einleitung

Dieses Anwenderszenario hilft Ihnen beim Umstieg von *Safety Matrix Viewer* V6.0/V6.1 auf *Safety Matrix Viewer* V6.2.

#### Voraussetzung

Voraussetzung ist ein übersetztes und geladenes Projekt.

#### Konsequenzen

- Keine Änderung des Sicherheitsprogramms
- Keine Änderung der Gesamtsignatur
- Übersetzen der OS erforderlich

### Vorgehensweise

1. Legen Sie vor der Installation der *Safety Matrix* V6.2 für den späteren Vergleich eine Sicherungskopie des gesamten S7-Projektes an.
2. Installieren Sie das *Safety MatrixAS-OS-Engineering* auf der ES.
3. Installieren Sie *Safety Matrix Viewer* auf der ES/OS sowie den entsprechenden Clients.
4. Starten Sie den **WinCC-Explorer** für die im Safety Matrix-Projekt enthaltene OS.
5. Öffnen Sie den **OS-Projekteditor** und klicken Sie auf **OK**. Das Projekt wird neu konfiguriert und damit das neue Bausteinsymbol übernommen.
6. Öffnen Sie den **Global Script C-Editor** und wählen Sie den Menübefehl **Optionen > Header neu generieren** an.
7. Führen Sie die Schritte unter "Bilder konvertieren" im Kapitel "Einbringen des neuen Safety Matrix-Bausteinsymbols in die PCS 7 OS (Seite 27)" aus.

Um das neue Bausteinsymbol auch in bereits vorhandene Anlagenbilder zu übernehmen, müssen Sie das jeweilige Projekt neu kompilieren.
Projektieren Sie ggf. die gewünschten Berechtigungen an den Bausteinsymbolen.

1. Starten Sie den *SIMATIC Manager*.
2. Stellen Sie sicher, dass in den Objekteigenschaften des betreffenden Bildobjektes im Register "Bausteinsymbole" die Option "Bausteinsymbole aus der Technologischen Hierarchie ableiten" aktiviert ist. (Dies ist bei *PCS 7* ab V7 voreingestellt.)
3. Markieren Sie das OS-Objekt und wählen Sie aus dem Kontextmenü "Übersetzen", um die OS zu übersetzen.

   Für *PCS 7* < V7: Stellen Sie sicher, dass im Assistent "OS Übersetzen" beim Wählen der Übersetzungsdaten und des Übersetzungsumfangs die Option "Bausteinsymbole erzeugen/aktualisieren" aktiviert ist. (Dies erfolgt bei *PCS 7* ab V7 automatisch.)
4. Betätigen Sie im letzten Dialog des Assistenten "OS Übersetzen" die Schaltfläche "Übersetzen".
5. Wiederholen Sie diese Schritte für alle Projekte.

### Ergebnis

Nachdem Sie diese Schritte durchgeführt haben, enthält Ihr Projekt das neue Safety Matrix-Bausteinsymbol.

# 3 Software-Oberfläche

## 3.1 Einfügen einer neuen Safety Matrix

### Matrix-Objekt

In einem SIMATIC-Projekt ist die Cause/Effect-Logik in einem Safety Matrix-Objekt hinterlegt, in dem die Logik eingerichtet und in Form von Funktionsbausteinen in einen *CFC*-Plan übertragen wird. Jedes Safety Matrix-Objekt unterstützt bis zu 128 Causes und 128 Effects mit maximal 1024 Schnittpunkten. Eine F-CPU kann mehrere Matrizen im Rahmen ihrer Speicherkapazität unterstützen.

### Hinzufügen eines Safety Matrix-Objekts in einem Projekt

1. Öffnen Sie den *SIMATIC Manager* und aktivieren Sie die Komponentensicht.
2. Öffnen Sie das Projekt im *SIMATIC Manager*.
3. Gehen Sie im Projekt zum S7-Programmordner.
4. Klicken Sie mit der rechten Maustaste auf den S7-Programmordner und wählen Sie **Neues Objekt einfügen > Matrixordner.** Ein neuer Safety Matrix-Ordner "Matrizen" wird im S7-Programm angelegt.
5. Klicken Sie mit der rechten Maustaste auf den Ordner "Matrizen" und wählen Sie die **Objekteigenschaften** des Matrixordners.
6. Geben Sie nach Wunsch im Register "Allgemein" einen Namen für den Matrixordner ein (max. 24 Zeichen), einen Autor (max. 40 Zeichen) und einen Kommentar (max. 254 Zeichen).
7. Klicken Sie mit der rechten Maustaste auf den Matrixordner und wählen Sie **Neues Objekt einfügen > Matrix**.
8. Geben Sie einen Namen (bis zu 24 Zeichen) für das Safety Matrix-Objekt ein. Bitte achten Sie bei der Namensvergabe darauf, dass der Name anlagenweit eindeutig ist. Groß-/Kleinschreibung wird nicht beachtet.

---

**Hinweis**

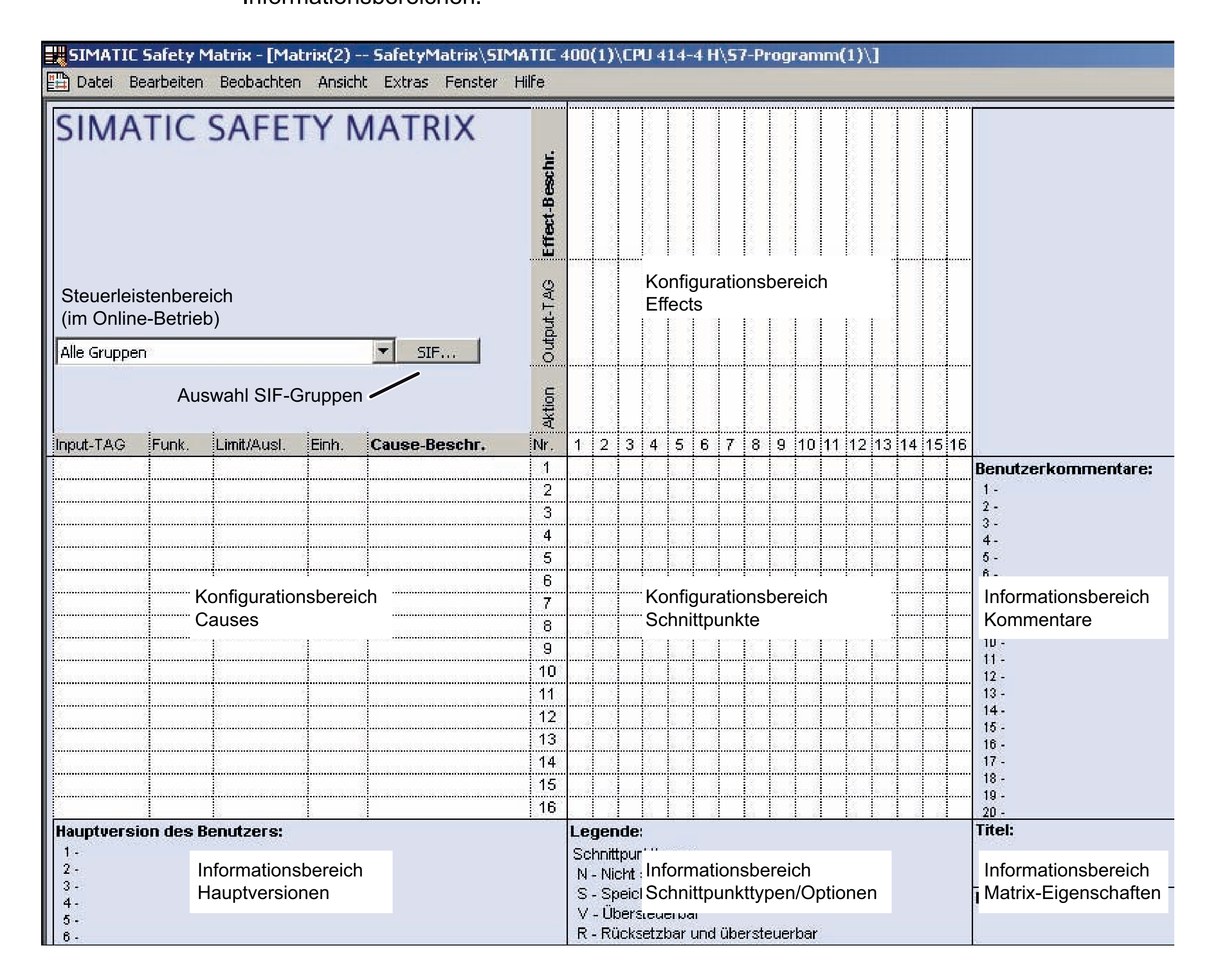
Um eine Safety Matrix zu kopieren, speichern Sie eine bestehende Safety Matrix mit dem *Safety Matrix Engineering Tool* unter einem anderen Namen ab (Menübefehl **Datei > Speichern als**) und importieren sie anschließend in dem vorgesehenen Safety Matrix-Ordner. Hierzu gehen Sie vor, wie im Kapitel "Importieren einer Cause/Effect-Matrixdatei (.cem) in ein PCS 7-Projekt (Seite 105) " beschrieben.

---

9. Doppelklicken Sie auf das Safety Matrix-Objekt im *SIMATIC Manager*.

## Ergebnis

Das *Safety Matrix Engineering Tool* öffnet die Safety Matrix. Das folgende Bild zeigt die Oberfläche einer Safety Matrix mit hervorgehobenen Konfigurations- und Informationsbereichen.




## Log-Fenster

Ein weiterer wichtiger Bestandteil der Safety Matrix-Oberfläche ist das Log-Fenster, das sich öffnet und aktiv wird zur Anzeige von:

- Konfigurationsreport
- Validierungsreport
- Ereignisprotokoll

Standardmäßig ist das Log-Fenster unterhalb der Safety Matrix angeordnet, Sie können es aber beliebig verschieben und in der Größe verändern.
Ist das Log-Fenster aktiviert, steht Ihnen eine reduzierte Menüleiste zur Verfügung, die Ihnen die Windows-üblichen Befehle zum Speichern, Drucken, Anordnen von Fenstern und Hilfe anbietet.

### Statuszeile

Die Statuszeile der Safety Matrix ist im Online- und Offline-Betrieb unterschiedlich:

- Im Offline-Betrieb enthält die Statuszeile einen Bereich für Statusanzeige und einen Bereich für Fehleranzeige.
- Im Online-Betrieb enthält die Statuszeile einen Bereich für Statusanzeige, einen Bereich für Fehleranzeige und zusätzlich eine Datum-/Uhrzeitanzeige.

### Name einer Safety Matrix muss eindeutig sein




**Geben Sie einer Safety Matrix einen eindeutigen Namen**

Sie müssen jeder Safety Matrix einen anlagenweit eindeutigen Namen geben, damit die Online-Kommunikation während einer Secure Write-Transaktion ausreichend abgesichert ist.

## 3.2 Die Menüleiste der Safety Matrix

### Übersicht Menüleiste

Die Menüleiste der Safety Matrix enthält die folgenden Menübefehle:

- Datei
- Bearbeiten
- Beobachten
- Ansicht
- Extras
- Fenster
- Hilfe

Im Folgenden werden die jeweiligen Unterbefehle der Menübefehle erläutert.

---

**Hinweis**

Es werden alle Menübefehle mit ihren Unterbefehlen aufgeführt, die im *Safety Matrix Engineering Tool* vorhanden sind. Zu den Einschränkungen im Funktionsumfang beim *Safety Matrix Editor* siehe Kapitel "Safety Matrix Editor (Seite 107)".

---

## Der Menübefehl "Datei"

Mit den Befehlen dieses Menübefehls bearbeiten Sie eine Safety Matrix-Datei, aber noch kein Safety Matrix-Objekt im *SIMATIC Manager*. Um die Safety Matrix im *SIMATIC Manager* zu verwenden, müssen Sie die Datei anschließend importieren.




**Bearbeiten der Safety Matrix-Datei**

Die .cem-Dateien dürfen Sie ausschließlich mit dem *Safety Matrix Engineering Tool* oder dem *Safety Matrix Editor* bearbeiten.

| Befehl | Funktion |
|---|---|
| Neu | Öffnet eine leere Safety Matrix unter dem Namen "NewMatrix.cem" als Readonly-Datei. Mit **Speichern** kann der neuen Safety Matrix ein Dateiname zugeordnet werden. |
| Öffnen... | Zeigt den Dialog **Öffnen** zur Auswahl und zum Öffnen einer zuvor projektierten Safety Matrix. Mit dieser Option kann eine Safety Matrix zum Bearbeiten geöffnet werden. |
| Schließen | Schließt die aktuelle Safety Matrix-Datei. Sie werden aufgefordert, Änderungen in der Safety Matrix zu speichern, bevor die Datei geschlossen wird. |
| Speichern | Speichert die aktuelle Safety Matrix in einer Datei. Werden Änderungen der Safety Matrix gespeichert, so ersetzt die neue Safety Matrix die ältere Version. Wird eine Safety Matrix in einem Projekt überschrieben, so werden Sie aufgefordert, die Log-Datei zu überprüfen und festzulegen, welche Änderungen Sie akzeptieren wollen (Kritisch/Nicht kritisch). Ebenso werden Sie aufgefordert, das Passwort für das Sicherheitsprogramm einzugeben. Beim Speichern in einer neuen Datei ist kein Passwort erforderlich. |
| Speichern als... | Speichert die Safety Matrix in einer anderen .cem-Datei. |
| Transferieren | Hiermit transferieren Sie die Safety Matrix in das Projekt. Siehe Kapitel "Safety Matrix transferieren (Seite 111)". |
| Drucken... | Öffnet den Dialog "Drucken". Im Dialog "Drucken " kann der Ausdruck der aktuellen Safety Matrix spezifiziert und veranlasst werden. Der Befehl **Drucken** steht nur im Offline-Betrieb zur Verfügung. |
| Druckvorschau | Zeigt eine Vorschau der Datei, die ausgedruckt werden soll. |
| Seite einrichten... | Der Dialog "Seite einrichten" bietet Ihnen mehrere Optionen zum Einrichten der auszudruckenden Seiten. |
| Letzte Dateien | Der Befehl **Letzte Dateien** bietet Ihnen die zuletzt aufgerufenen Safety Matrix-Dateien namentlich zur Auswahl an. |
| Beenden | Schließt alle Dialogfelder und beendet das Programm. Befehl **Beenden** steht nur im Offline-Betrieb zur Verfügung. |

## Der Menübefehl "Bearbeiten"

| Befehl | Funktion |
|---|---|
| Eigenschaften | Der Dialog "Eigenschaften" bietet Ihnen umfangreiche Informationen und Eingabemöglichkeiten bezüglich der allgemeinen Eigenschaften der Safety Matrix. Siehe Kapitel "Der Dialog "Eigenschaften" der Safety Matrix (Seite 75) ". |
| Alles löschen | Löscht die gesamte Safety Matrix, einschließlich der Versionshistorie, Kommentare, etc. Außerdem wird die Größe der Safety Matrix auf 16 Causes und 16 Effects zurückgesetzt. |

## Der Menübefehl "Beobachten"

| Befehl | Funktion |
|---|---|
| Konfigurieren... | Im Dialog "Konfigurieren" können Sie die Zeit in Sekunden für den Beobachtungszyklus angeben, also die Zykluszeit für die Aktualisierung der Oberfläche. |
| Beobachten Ein/Aus | Hiermit schalten Sie den Online-Betrieb ein bzw. aus. |

## Der Menübefehl "Ansicht"

| Befehl | Funktion |
|---|---|
| Anpassen | Öffnet die Dialoge "Anpassen - Layout" und "Anpassen - Farben". Diese Dialoge bieten Ihnen umfangreiche Möglichkeiten zum Anpassen des Erscheinungsbildes und der angezeigten Informationen in der Safety Matrix. Siehe Kapitel "Die Dialoge "Anpassen" (Seite 80) ". |
| Aktualisieren bzw. <F5> | Erzwingt ein Neuzeichnen der aktuellen Safety Matrix. Mit dieser Funktion können Änderungen in der Symboltabelle und im Sicherheitsprogramm, die bei geöffneter Safety Matrix vorgenommen wurden, übernommen werden. Ebenso kann die Zellenbreite der Cause- und Effect-Zellen anhand der längsten eingegebenen Zeichenketten in der Größe angepasst werden. |

## Der Menübefehl "Extras"

| Befehl | Funktion |
|---|---|
| CFC | Hiermit übersetzen Sie das SIMATIC-Projekt. Siehe Kapitel "Übersetzen und Laden (Seite 121) ". |
| CPU | Hier laden Sie das SIMATIC-Projekt in das Automatisierungssystem. Siehe Kapitel "Übersetzen und Laden (Seite 121) ". |
| Änderungs-verfolgung | Wenn Sie den Befehl **Änderungen akzeptieren** wählen, werden Sie aufgefordert, die Log-Datei zu überprüfen und festzulegen, welche Änderungen Sie akzeptieren wollen (Kritisch/Nicht kritisch).<br>Außerdem können Sie festlegen, ob Änderungen beim Speichern bzw. beim Speichern-als automatisch akzeptiert werden. |
| Vergleiche Matrix mit | Hier können Sie die Safety Matrix mit anderen Safety Matrizen vergleichen. Siehe Kapitel "Safety Matrizen vergleichen (Seite 153) ". |
| Vergleiche Programme... | Mithilfe des Dialogs "Vergleiche Programme" können Sie alle *CFC*-Pläne eines Planordners, die vom *Safety Matrix Engineering Tool* beim Transfer erzeugt werden, miteinander vergleichen und Abweichungen anzeigen und ausdrucken. Siehe Kapitel "CFC-Pläne vergleichen (Seite 154) ". |
| Reporte | • **Konfigurationsreport** erzeugt einen Bericht mit der kompletten Safety Matrix-Konfiguration im Log-Fenster.<br>• **Validierungsreport** startet eine Plausibilitätsprüfung der Safety Matrix-Konfiguration und zeigt die Ergebnisse im Log-Fenster.<br>• **Letzter Report** öffnet das Log-Fenster und platziert den Cursor in dem letzten Report (Konfigurationsreport, Validierungsreport, Ereignisprotokoll). Diese Informationen werden jeweils von den aktuellsten Vorgängen überschrieben.<br>Wählen Sie bei aktivem Log-Fenster den Menübefehl **Datei > Speichern als**, um die angezeigten Daten zu speichern. |

## Der Menübefehl "Fenster"

| Funktion |
|---|
| Hier stehen Ihnen die Windows-üblichen Befehle zur Anzeige mehrerer Fenster und zum Anzeigen aktuell geöffneter Safety Matrizen zur Verfügung. |

## Der Menübefehl "Hilfe"

| Befehl | Funktion |
|---|---|
| Inhalt | Öffnet das Inhaltsverzeichnis der Hilfe. |
| Benutzerhand-buch (PDF) | Öffnet die PDF-Datei des Benutzerhandbuchs. |
| Über... | Zeigt Versionsinformationen über das Safety Matrix-Programm an. |

# 4 Projektieren

## 4.1 Übersicht zum Projektieren

### 4.1.1 Prinzipielle Vorgehensweise zum Erstellen eines Sicherheitsprogramms

#### Einleitung

Auf Basis der gängigen Cause/Effect-Methode ermöglicht die Safety Matrix eine einfache Projektierung, bei der Sie auftretenden Ereignissen (Causes) exakt definierte Reaktionen (Effects) zuordnen und damit das Systemverhalten der Anlage festlegen. Dabei bietet Ihnen die Safety Matrix umfangreiche Unterstützung durch:

- Strukturierte Benutzeroberfläche
- Einfache Parametrierung und Verknüpfung der Causes und Effects
- Automatische Prüfung der Projektierung auf Plausibilität
- Automatische Platzierung der F-Kanaltreiber während des Transfers in einen *CFC*-Plan
- Automatische Generierung der F-Systems-Programmlogik auf *CFC*-Basis mit F-Bausteinen aus der Safety Matrix-Bibliothek
- Versions- und Änderungsverfolgung, Funktionen zum Vergleichen von Matrizen und zur Unterstützung bei der Abnahme der Anlage

#### Voraussetzungen

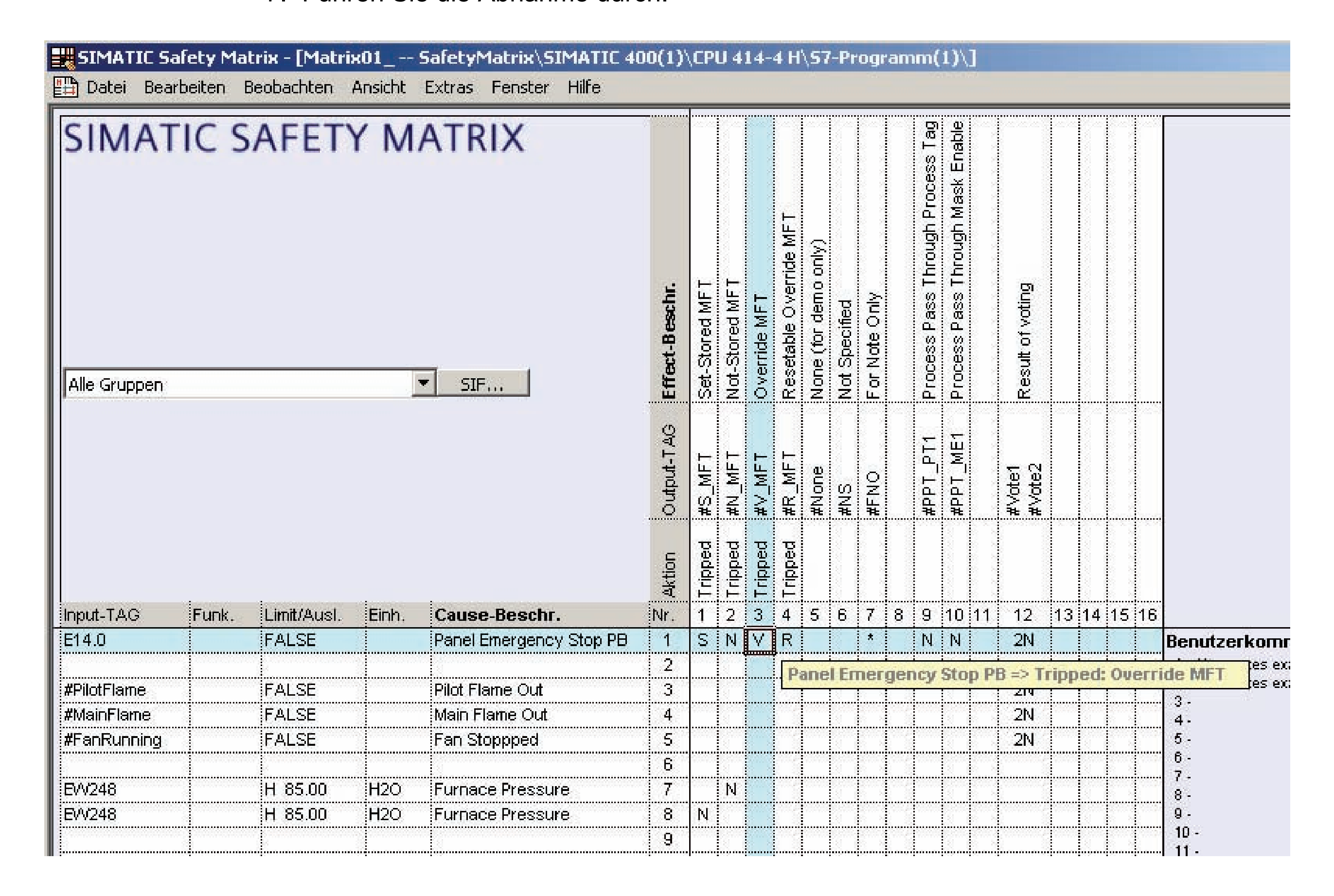
- Sie müssen eine Projektstruktur im *SIMATIC Manager* angelegt haben.
- Ihr Sicherheitsprogramm müssen Sie einer F-fähigen Zentralbaugruppe, z. B. einer CPU 412-3H, CPU 414-4H oder CPU 417-4H zugeordnet haben.
- Für die F-CPU muss die Option "CPU enthält Sicherheitsprogramm" aktiviert und ein Passwort für die F-CPU vergeben worden sein.
- Sie müssen die Ein- und Ausgänge in *HW Konfig* bzw. der Symboltabelle im *SIMATIC Manager* konfiguriert haben. Die Safety Matrix arbeitet mit den symbolischen Namen der Eingänge (Input-TAGs) und Ausgänge (Output-TAGs) der F-Baugruppen.

#### Prinzipielle Vorgehensweise

Gehen Sie zum Erstellen eines Sicherheitsprogramms folgendermaßen vor:

1. Nachdem Sie die Programmstruktur festgelegt haben, fügen Sie eine Safety Matrix in das Projekt ein.

2. Fügen Sie die
   - Input-TAGs für Causes und
   - Output-TAGs für Effects in die Safety Matrix ein
3. Parametrieren Sie
   - Causes
   - Effects
   - Schnittpunkte
4. Transferieren Sie die Safety Matrix in *CFC*-Pläne.
5. Übersetzen und laden Sie das S7-Programm.
6. Testen und dokumentieren Sie das Sicherheitsprogramm.
7. Führen Sie die Abnahme durch.



### 4.1.2 Die TAGs der Safety Matrix

#### Welche TAGs unterstützt die Safety Matrix?

Folgende TAGs werden von der Safety Matrix unterstützt:

- Input- und Output-TAGs; diese bilden die Schnittstelle der Safety Matrix zur F-Peripherie. Die Input- und Output-TAGs umfassen die symbolischen Namen der im SIMATIC-Projekt konfigurierten Ein- und Ausgänge der SIMATIC F-Baugruppen und die zugeordneten F-Kanaltreiber
- beliebige Signale aus dem Sicherheitsprogramm über Anschlüsse am hierarchischen Plan
- Zustand eines Cause, Effect oder Effect-TAG über interne Referenzen
- kundenspezifische F-Kanaltreiber

#### Einbindung der TAGs in die Safety Matrix

Im Dialog "Cause Details", Register "Konfigurieren", Schaltfläche "I/O", stehen Ihnen die folgenden Optionen für die Einbindung von TAGs in die Safety Matrix zur Verfügung (siehe Kapitel Dialog "Cause-Details" - Register "Konfigurieren" (Seite 87)").

**Option "Externer Anschluss" (Präfix "#")**

Soll ein Cause oder Effect mit einem **beliebigen Signal aus dem Sicherheitsprogramm** verschaltet werden, so müssen Sie bei der Projektierung des TAG eine der folgenden Optionen wählen:

- Bei Input-TAGs (Causes oder z. B. Bypass-TAG) wird ein Plan**eingang** am hierarchischen Plan der Matrixlogik angelegt (zur Versorgung aus *CFC*).
- Bei Output-TAGs (Effects) wird ein Plan**ausgang** am hierarchischen Plan der Matrixlogik angelegt (zur Verarbeitung des Effect-TAG im *CFC*).

**Option "Interne Referenz" ("Cause[x]", "Effect[x]" bzw. "Effect[x][y]")**

Der Zustand eines Cause, Effect oder Effect-TAG innerhalb der Safety Matrix kann an einem Input-TAG weiterverarbeitet werden. Dafür müssen Sie "Cause[x]" bzw. "Effect[x](TAG)[y]" auswählen.

**Option "Kanaltreiber" (Safety Matrix-eigene Input- und Output-TAGs)**

Das *Safety Matrix Engineering Tool* platziert für Input- und Output-TAGs automatisch F-Kanaltreiber von SIMATIC F-Baugruppen. Dies erfolgt während des Transfers in einen *CFC*-Plan, wenn für die jeweiligen F-Kanäle kein F-Kanaltreiber von SIMATIC F-Baugruppen existiert.

- **Option "Kanaltreiber - mit Überwachung" (Suffix "#")**

  Es wird wie bei Input- und Output-TAGs immer ein F-Kanaltreiber im hierarchischen Plan der Kanaltreiber angelegt.
  **Zusätzlich** wird

  – bei Input-TAGs ein Plan**ausgang** am hierarchischen Plan der Kanaltreiber angelegt (zur Weiterverarbeitung des gelesenen Treibersignals im *CFC*, zusätzlich zur Verarbeitung in der Safety Matrix)

  – bei Output-TAGs ein Plan**ausgang** am hierarchischen Plan der Matrixlogik angelegt (zur Weiterverarbeitung des Effects im *CFC*, zusätzlich zur Ausgabe an den F-Kanaltreiber).

Sind sowohl Präfix "#" als auch Suffix "#" angegeben, so wird beim Transfer der Suffix entfernt.

- **Option "Kanaltreiber - extern verwendet" (Präfix "@")**

Wurde der Input-/Output-TAG bereits von einer anderen Safety Matrix oder Benutzerlogik projektiert, so führt die transferierte Safety Matrix eine Verschaltung mit dem vorhandenen F-Kanaltreiber aus. Eine solche Verschaltung mit einem vorhandenen F-Kanaltreiber wird vom *Safety Matrix Engineering Tool* automatisch mit einem vorangestellten "@" im Projektierungsfeld des TAG gekennzeichnet, und das Häkchen im Kontrollkästchen "extern verwendet" wird gesetzt.

---

**Hinweis**

Falls der F-Kanaltreiber von SIMATIC F-Baugruppen mit dem angegebenen TAG während des Safety Matrix-Transfers nicht existiert, so wird das Präfix entfernt, und der TAG wird als Safety Matrix-eigener Input-/Output-TAG behandelt. Ebenso wird das Präfix beim Transfer automatisch hinzugefügt, falls der F-Kanaltreiber schon in einer anderen Safety Matrix existiert.

---

- **Option "Kanaltreiber - kundenspezifischer" (Präfix "~")**

Sie können Causes und Effects mit den Signalen von kundenspezifischen F-Kanaltreibern verschalten. Eine solche Verschaltung mit einem kundenspezifischen F-Kanaltreiber wird vom *Safety Matrix Engineering Tool* automatisch mit einer vorangestellten "~" im Projektierungsfeld des TAG gekennzeichnet.
Siehe auch Kapitel "Kundenspezifische F-Kanaltreiber (Seite 59)".

- **Option "Kanaltreiber - mit Vorverarbeitung" (Präfix "*")**

Sie können für diskrete und analoge Input-TAGs eine Vorverarbeitung verschalten. Eine solche Verschaltung mit einer Vorverarbeitung wird vom *Safety Matrix Engineering Tool* nach dem Transfer mit einem vorangestellten "*" im Projektierungsfeld des TAG gekennzeichnet.
Siehe auch Kapitel "Vorverarbeitung (Seite 57)".

### 4.1.3 Syntaxregeln für TAG-Namen in der Safety Matrix

#### Arten von TAG-Namen

In der Safety Matrix sind die folgenden Arten von TAG-Namen möglich:

- Safety Matrix-eigener Input- bzw. Output-TAG
- beliebige Signale aus dem Sicherheitsprogramm
- interne Referenzen ("Cause[x]", "Effect[x]", "Effect[x][y]")
- kundenspezifische F-Kanaltreiber

#### Zulässige Zeichen

Grundsätzlich sind nur ASCII-Zeichen im Bereich von 16#20 (Leerzeichen) bis 16#7a (kleines "z") erlaubt. Alle anderen Zeichen werden schon bei der Eingabe ignoriert. Außerdem werden auch die beiden Zeichen 16#2f ("/") und 16#5c ("\") ignoriert.

| ACHTUNG |
|---|
| Bei Eingabe der ignorierten Zeichen werden diese verworfen, es erscheint **keine** Fehlermeldung oder Warnung. Sie müssen sofort bei der Eingabe kontrollieren, ob der TAG-Name auch korrekt übernommen wurde, andernfalls kann es zu Übersetzungsfehlern (Symbol nicht definiert) oder gar Kollisionen mit bereits vorhandenen Symbolen kommen. |

Buchstaben sind sowohl als Großbuchstaben als auch Kleinbuchstaben möglich, allerdings wird die Groß-/Kleinschreibung nicht beachtet, d. h. die Symbole "TIC2344", "TiC2344" und "tic2344" sind identisch. Ausnahme sind hier die internen Referenzen, siehe unten.

## Safety Matrix-eigener Input-/Output-TAG

Maximale Anzahl der Zeichen: 24.

Safety Matrix-eigene Input-/Output-TAGs sind TAGs, die beim Transfer in einen *CFC*-Plan komplett von der Safety Matrix verschaltet werden (evtl. auch mittels IEA-Support, siehe Kapitel "Safety Matrix transferieren (Seite 111)").

Für einen Safety Matrix-eigenen TAG dürfen folgende Zeichen verwendet werden:

- Sonderzeichen: !$&()*+,- :;<=>? []^_`
- Ziffern: 0123456789
- Großbuchstaben: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Kleinbuchstaben: abcdefghijklmnopqrstuvwxyz

Folgende Sonderzeichen dürfen **nicht** verwendet werden:

- " (Anführungsstriche)
- . (Punkt)
- % (Prozent)
- ~ (Tilde)

Folgende Sonderzeichen dürfen nicht in allen Positionen verwendet werden:

- (Leerzeichen): Darf nicht am Anfang und nicht am Ende eines Symbols stehen.
- # (Hash): Darf nicht am Anfang und nicht am Ende eines Symbols stehen, da es hier zur Kennzeichnung als Plananschluss dient.
- ' (Hochkomma): Darf nicht am Ende eines Symbols stehen.
- @ (Klammeraffe): Darf nicht am Anfang eines Symbols stehen, da es hier zur Kennzeichnung als externe Adresse dient.

## Beliebige Signale aus dem Sicherheitsprogramm

Maximale Anzahl der Zeichen (Präfix/Suffix nicht mitgezählt): 24.

Für Plan-Eingänge gelten im *CFC* besondere Syntaxregeln, die dadurch auch für alle TAGs mit dem Präfix oder Suffix "#" gelten:

- Am Anfang des Namens dürfen nur Buchstaben (bei Suffix "#") bzw. Buchstaben oder der Unterstrich stehen (bei Präfix "#").
- Innerhalb des Namens sind nur Buchstaben, Ziffern und der Unterstrich erlaubt.
- Der Unterstrich darf nicht mehrfach hintereinander verwendet werden.
- Der Unterstrich darf nicht am Anfang (bei Suffix "#") und nicht am Ende des Namens verwendet werden.

### Beispiele für gültige Plananschlussnamen

- #TIC4711
- #TIC_4711
- #_4_321

### Beispiele für ungültige Plananschlussnamen

- #4711 (Ziffer am Anfang)
- #TIC__543 (Unterstrich mehrfach verwendet)
- #TIC_4711_ (Unterstrich am Ende)
- _TIC_4711# (Unterstrich am Anfang bei Suffix "#")

### Interne Referenzen ("Cause[x]", "Effect[x]", "Effect[x][y]")

Interne Referenzen wählen Sie menügesteuert aus.

## 4.1.4 Vorverarbeitung

### Vorverarbeitung für Input-TAGs

Sie können für diskrete und analoge Input-TAGs eine Vorverarbeitung verschalten.

Bei der Vorverarbeitung handelt es sich um einen *CFC*-Plan, den Sie selber erstellen können, z. B. um eine Rechenfunktion für die Umrechnung von Druck in Temperatur. Der Vorverarbeitungs-Plan muss innerhalb der "SafetyMatrix Lib (V1_3)" in den Ordner "Templates" eingebracht worden sein und den folgenden Regeln entsprechen.

- Template für analoge Vorverarbeitung:

| REAL | |
|---|---|
| V_IN | Eingang Prozesswert |
| V_OUT | Ausgang Prozesswert |
| SIM_V_IN | Eingang Simulationswert |
| SIM_V_OUT | Ausgang Simulationswert |

In den Eigenschaften des Vorverarbeitungs-Plans muss ein Kommentar eingetragen sein, der mit "SM_REAL_..." beginnt.

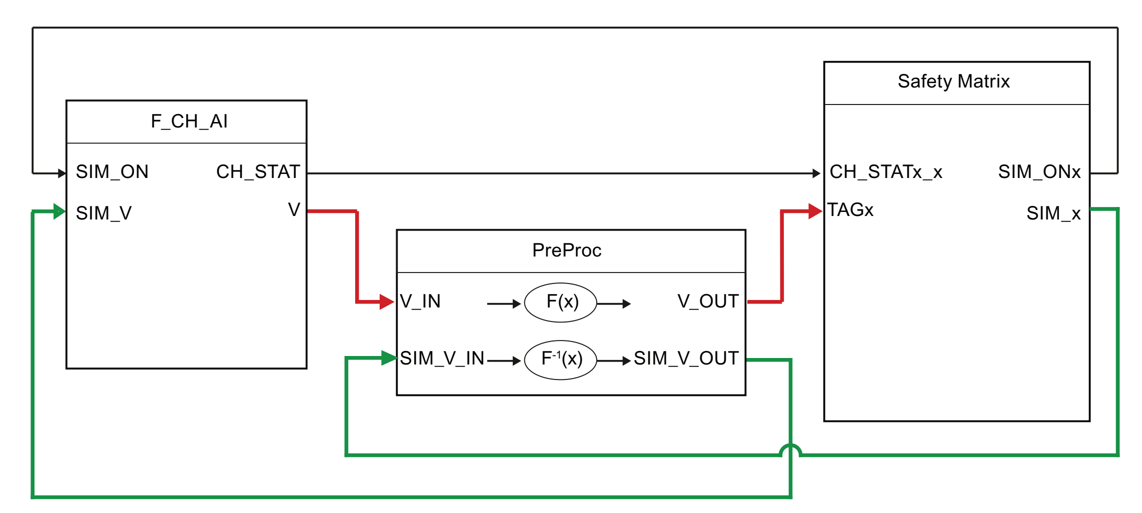
- Template für diskrete Vorverarbeitung:

| BOOL | |
|---|---|
| Q_IN | Eingang Prozesswert |
| Q_OUT | Ausgang Prozesswert |
| SIM_I_IN | Eingang Simulationswert |
| SIM_I_OUT | Ausgang Simulationswert |

In den Eigenschaften des Vorverarbeitungs-Plans muss ein Kommentar eingetragen sein, der mit "SM_BOOL_..." beginnt.

Eine Vorverarbeitung ist möglich für Input-TAGs mit der Option "Kanaltreiber" bzw. "Kanaltreiber - kundenspezifischer".

Das folgende Bild zeigt das Prinzip der Vorverarbeitung anhand eines analogen Input-TAG.




Für die Vorverarbeitung wird ein eigener hierarchischer Plan "PP_Chart" im hierarchischen Plan der Matrixlogik angelegt. In diesem Plan "PP_Chart" wird für jede Vorverarbeitung ein eigener hierarchischer Plan angelegt. Diese hierarchischen Pläne können Sie bearbeiten, sie dürfen jedoch nicht verschoben werden!

Durch den Einbau der Funktion $F^{-1}(x)$ kann in der Safety Matrix ausschließlich mit den vorverarbeiteten Werten gearbeitet werden.
So können Sie z. B. beim Simulieren Werte aus dem Wertebereich der vorverarbeiteten Signale vorgeben, die $F^{-1}(x)$-Funktion rechnet diese zurück und am Kanaltreiber sind somit die Signale im Wertebereich des Kanaltreibers verfügbar.

---

**Hinweis**

Die "SafetyMatrix Lib (V1_3)" enthält im Ordner "Templates" zwei Vorverarbeitungs-Pläne ohne interne Funktionalität, die Sie kopieren bzw. nach Wunsch anpassen können.

---

### 4.1.5 F-Kanaltreiber

#### F-Kanaltreiber in die Safety Matrix einbinden

Die Safety Matrix V6.2 bietet Ihnen verschiedene Möglichkeiten, F-Kanaltreiber in die Safety Matrix einzubinden. Die folgende Tabelle enthält eine Übersicht, auf welche Art und Weise Sie dies erreichen können.

| Kanaltreibertyp | Einbindung | Version | | |
|---|---|---|---|---|
| | | V5.2 | V6.1 | V6.2 |
| F_CH_AI<br>F_CH_DI<br>F_CH_DO | Die F-Kanaltreiber werden:<br>• beim Transfer im hierarchischen Plan der F-Kanaltreiber platziert und verschaltet<br>• vorab mittels IEA Unterstützung platziert und beim Transfer verschaltet | X | X<br>X | X<br>X |
| F_CH_BI<br>F_CH_BO | Die F-Kanaltreiber werden:<br>• vorab mittels IEA Unterstützung platziert und beim Transfer verschaltet | | X | X |
| F_CH…*<br>F_PA…<br>F_Q…<br>F-Typicals | Die F-Kanaltreiber werden:<br>• vorab platziert und mittels Option "kundenspezifisch" eingebunden | | | X |

*) nicht jedoch die explizit genannten F_CH_AI, F_CH_DI/DO, F_CH_BI/BO

## Kundenspezifische F-Kanaltreiber

Ein F-Baustein wird als kundenspezifischer F-Kanaltreiber erkannt, wenn er ins Sicherheitsprogramm eingebracht wurde und einer der folgenden beiden Punkte erfüllt ist:

- Es handelt sich um einen F-Systems F-Baustein vom Typ
  - F_CH... (nicht jedoch F_CH_AI, F_CH_DI/DO, F_CH_BI/BO)
  - F_PA...
  - F_Q...
- Es handelt sich um einen F-Bausteintyp bzw. einen F-Baustein mit folgenden Eigenschaften:
  - Er hat eine Schnittstelle wie folgt:

    - Eingangsparameter zum Einschalten der Simulation: SIM_ON

    - Eingangsparameter zur Vorgabe des Simulationswerts:
    SIM_I bei diskreten TAGs / SIM_V bei analogen TAGs

    - Ausgangsparameter Kanalstatus CH_STAT:
    mittels F_FBO_SM bilden, siehe unten

    - Parameter für Signalausgang bzw. -eingang:
    Q bei diskreten TAGs / V oder I bei analogen TAGs

    - Optional: Parameter ACK_REQ und ACK_REI zur Quittierung
  - der F-Bausteintyp enthält den F-Baustein F_FBO_SM.

---

**Hinweis**

Hat der Parameter SIM_V Ihres kundenspezifischen Kanaltreibers nicht den Datentyp REAL, wird er nach dem Transfer als "extern verwendet" (Präfix "@") gekennzeichnet. Wollen Sie diesen Kanaltreiber trotzdem simulieren, so können Sie sich einen F-Bausteintyp erstellen, der die entsprechende Datenwandlung enthält, und diesen in die Safety Matrix einbinden.

---

## F-Baustein F_FBO_SM

Mit Hilfe des F-Bausteins F_FBO_SM können Sie den Ausgangsparameter Kanalstatus CH_STAT für die Safety Matrix bilden. Dieser Ausgang wird benötigt, um einen F-Bausteintyp als kundenspezifischen F-Kanaltreiber einbinden zu können.

Achten Sie bei der Erstellung des Baustein-Typicals auf die Position des F_FBO_SM in der Ablaufreihenfolge. Dieser darf nicht an erster Stelle sein.

Folgende Informationen können über den Kanalstatus an die Safety Matrix übergeben werden:

- QBAD der F-Kanaltreiber
- QSIM der F-Kanaltreiber
- PASS_OUT der F-Kanaltreiber
- PROFIsafe-Fehler des Baugruppentreibers

### Anschlüsse des F-Bausteins F_FBO_SM

| | Name | Datentyp | Erklärung | Vorbesetzung |
|---|---|---|---|---|
| Eingänge: | QBAD | F_BOOL | 1 = Prozesswert ungültig | FALSE |
| | QSIM | F_BOOL | 1 = Simulation aktiv | FALSE |
| | PASS_OUT | F_BOOL | 1 = Passivierung wegen Fehler | FALSE |
| | PS_ERR | F_BOOL | 1 = Kommunikationsfehler PROFIsafe | FALSE |
| | | | | |
| Ausgänge: | CH_STAT | F_WORD | Kanalstatus für Safety Matrix | W#16#0 |

## 4.1.6 Meldungsprojektierung

### 4.1.6.1 Übersicht zum Projektieren der Meldungen

### Meldungsprojektierung für die Safety Matrix und für einzelne Causes und Effects

Sie können sowohl Meldungen für die gesamte Safety Matrix projektieren als auch Meldungen für einzelne Causes und Effects. Je nach Projektierung werden beim Transfer ins Projekt die folgenden Meldebausteine platziert:

- 1-mal der Meldebaustein F_MA_AL für die Safety Matrix
- x-mal der Meldebaustein F_SC_AL, jeweils für einen Cause
- x-mal der Meldebaustein F_SE_AL, jeweils für einen Effect

Es gibt unterschiedliche Alarm-Profile für:

- Meldungen einzelner Causes. Für Causes gibt es drei vordefinierte Alarm-Profile: "Standard", "Sequential", "Energized".
- Meldungen einzelner Effects. Für Effects gibt es zwei vordefinierte Alarm-Profile: "Standard", "Sequential".
- Meldungen der Safety Matrix
- Sammelmeldungen (Verknüpfung der Zustände aller Meldebausteine von Causes und Effects)

Diese Alarm-Profile können Sie wie folgt projektieren:

- einzelne Meldungen freigeben
- Meldeklassen ändern
- Prioritäten der Meldeklassen ändern
- die Quittieranforderung festlegen

## Anschlüsse der Meldebausteine

An den Meldebausteinen im *CFC* stehen Ihnen zusätzliche Informationen zur Weiterverarbeitung zur Verfügung. Ebenso können Sie Funktionen wie "Sperren der Alarme beim Hochlauf" im *CFC* projektieren. Siehe dazu die folgenden Kapitel:

Safety Matrix-Meldebaustein F_MA_AL (Seite 63)

Cause-Meldebaustein F_SC_AL (Seite 64)

Effect-Meldebaustein F_SE_AL (Seite 69)

## Syntaxregeln für Meldungsprojektierung

Sind Meldungen für Causes und Effects projektiert, wird die jeweilige Cause/Effect-Beschreibung in den Meldetext integriert. Achten Sie deshalb auf die Einhaltung der Syntaxregeln: Es sind 32 alphanumerische Zeichen erlaubt.

Siehe dazu die folgenden Kapitel:

Dialog "Cause-Details" - Register "Konfigurieren" (Seite 87)

Dialog "Effect-Details" - Register "Konfigurieren" (Seite 96)

Bei Nichteinhaltung werden die Fehler im Log-Fenster des Transfers aufgelistet und die Meldungsprojektierung wird nicht umgesetzt.

### 4.1.6.2 Safety Matrix-Meldebaustein F_MA_AL

#### Zusätzliche Informationen zur Weiterverarbeitung

Am Safety Matrix-Meldebaustein F_MA_AL im *CFC* stehen Ihnen zusätzliche Informationen zur Weiterverarbeitung zur Verfügung. Ebenso können Sie Funktionen wie "Sperren der Alarme beim Hochlauf" im *CFC* projektieren.

#### Anschlüsse des Safety Matrix-Meldebausteins F_MA_AL

| | Name | Datentyp | Erklärung |
|---|---|---|---|
| Eingänge | M_Name | String[16] | Matrix-Name |
| | MSG_LOCK | BOOL | 1= Sperren aller Alarme |
| | | | |
| Ausgänge | ACK_REQ | BOOL | Anforderung zur Quittierung von den Kanaltreibern |
| | SM_CHG | BOOL | Änderung der Matrix-Signatur oder der Version (Information steht nur einen Zyklus zur Verfügung) |
| | MatrixSIG | DWORD | Matrix-Signatur |
| | MtxVersion | STRING[20] | Fest eingestellte Version der Safety Matrix Library |
| | MajorRev | INT | Hauptversion der projektierten Matrix |
| | MinorRev | INT | Nebenversion der projektierten Matrix |
| | Any_CA | BOOL | 1= ein Cause der Matrix ist aktiv<br>0= kein Cause ist aktiv |
| | Any_EA | BOOL | 1= ein Effect der Matrix ist aktiv<br>0= kein Effect ist aktiv |
| | CAct_Num | INT | Anzahl der aktiven Causes |
| | EAct_Num | INT | Anzahl der aktiven Effects |
| | Any_CB | BOOL | 1= ein Cause der Matrix ist überbrückt (Bypass)<br>0= kein Cause ist überbrückt |
| | Any_EB | BOOL | 1= ein Effect der Matrix ist überbrückt (Bypass)<br>0= kein Effect ist überbrückt |
| | CByp_Num | INT | Anzahl der Causes mit Bypass |
| | EByp_Num | INT | Anzahl der Effects mit Bypass |
| | Any_CW | BOOL | 1= eine Cause-Vorwarnung aktiv<br>0= keine Cause-Vorwarnung aktiv |
| | Any_EW | BOOL | 1= eine Effect -Vorwarnung aktiv<br>0= keine Effect -Vorwarnung aktiv |
| | Msec | DINT | Aktuelle Matrix-Laufzeit, beinhaltet die Laufzeit aller Matrix-Bausteine und der Kanaltreiber |
| | MaxMsec | DINT | Bisher maximale Matrix-Laufzeit, beinhaltet die höchste Laufzeit aller Matrixbausteine und der Kanaltreiber |

#### Siehe auch

Cause-Meldebaustein F_SC_AL (Seite 64)

Effect-Meldebaustein F_SE_AL (Seite 69)

### 4.1.6.3 Cause-Meldebaustein F_SC_AL

## Zusätzliche Informationen zur Weiterverarbeitung

An den Cause-Meldebausteinen F_SC_AL im *CFC* stehen Ihnen zusätzliche Informationen zur Weiterverarbeitung zur Verfügung. Ebenso können Sie Funktionen wie "Sperren der Alarme beim Hochlauf" im *CFC* projektieren.

## Anschlüsse des Cause-Meldebausteins F_SC_AL

| | Name | Datentyp | Erklärung |
|---|---|---|---|
| Eingänge: | M_Name | String[16] | Matrix-Name |
| | Number | INT | Cause-Nummer |
| | MSG_LOCK | BOOL | 1=Sperren aller Alarme |
| | | | |
| Ausgänge | CONFIG_V | DWORD | Cause-Konfiguration; siehe unten: Tabelle "CONFIG_V" |
| | STATE_V | DWORD | Cause-Status; siehe unten: Tabelle "STATE_V" |
| | DIAG_V | DWORD | Cause-Fehler; siehe unten: Tabelle "DIAG_V" |
| | P_LIM_V | REAL | Projektierte Vorwarnungsgrenze für Analogwerte; bei Überschreitung dieses Wertes wird eine Vorwarnung ausgegeben |
| | LIMIT_V | REAL | Projektierte Grenze für Analogwerte; bei Überschreitung dieses Wertes löst der Analog-TAG aus |
| | HYST_V | REAL | Projektierte Hysterese für die Auslösung des Analog-TAG bzw. für das Rücknehmen der Auslösung |
| | DELTA_V | REAL | Projektierte Diskrepanz, welche zwischen den Werten der Analog-TAGs zugelassen ist |
| | DELAY_V | DINT | Projektierter Zeitwert für die Zeitverzögerung zur Auslösung von Causes in ms |
| | TAG1_R | REAL | Analogwert TAG1, der in der Safety Matrix bearbeitet wird |
| | TAG2_R | REAL | Analogwert TAG2, der in der Safety Matrix bearbeitet wird |
| | TAG3_R | REAL | Analogwert TAG3, der in der Safety Matrix bearbeitet wird |
| | VMOD1_R | REAL | Eingelesener Analogwert über die Baugruppe für TAG1 |
| | VMOD2_R | REAL | Eingelesener Analogwert über die Baugruppe für TAG2 |
| | VMOD3_R | REAL | Eingelesener Analogwert über die Baugruppe für TAG3 |
| | TAG1_B | BOOL | Diskreter Wert TAG1, der in der Safety Matrix bearbeitet wird |
| | TAG2_B | BOOL | Diskreter Wert TAG2, der in der Safety Matrix bearbeitet wird |
| | TAG3_B | BOOL | Diskreter Wert TAG3, der in der Safety Matrix bearbeitet wird |
| | VMOD1_B | BOOL | Eingelesener Wert über die Baugruppe für TAG1 |
| | VMOD2_B | BOOL | Eingelesener Wert über die Baugruppe für TAG2 |
| | VMOD3_B | BOOL | Eingelesener Wert über die Baugruppe für TAG3 |
| | TAG_TYPE | BOOL | Konfiguration TAG:<br>1= analoger TAG<br>0= diskreter TAG |
| | ACK_REQ | BOOL | 1= Quittierungsanforderung |

| | Name | Datentyp | Erklärung |
|---|---|---|---|
| | FIRSTOUT | BOOL | First Out-Alarm; 1= wenn der Cause der erste ausgelöste Cause seiner FO-Gruppe ist |
| | ACTIVE | BOOL | 1= Cause hat ausgelöst<br>0= Cause hat nicht ausgelöst |
| | ANY_BYP | BOOL | Umgehung aktiv; 1= wenn eine der folgenden Umgehungen aktiv ist: (Hard-)Bypass, Soft-Bypass, Unterdrückung, Simulation eines TAG |
| | PRE_AL | BOOL | Vorwarnung aktiv; 1= wenn ein analoger TAG des Cause die projektierte Vorwarnungsgrenze (P_LIM_V) überschritten hat |
| | ANY_DIAG | BOOL | 1= wenn Diagnosemeldungen vorliegen (DIAG_V nicht 0) |
| | CH_STAT1 | WORD | Wenn der TAG mit einem Kanaltreiber verbunden ist, wird hier der Kanalstatus angezeigt (TAG1); siehe unten: Tabelle "CH_STATx" |
| | CH_STAT2 | WORD | Wenn der TAG mit einem Kanaltreiber verbunden ist, wird hier der Kanalstatus angezeigt (TAG2 ); siehe unten: Tabelle "CH_STATx" |
| | CH_STAT3 | WORD | Wenn der TAG mit einem Kanaltreiber verbunden ist, wird hier der Kanalstatus angezeigt (TAG3 ); siehe unten: Tabelle "CH_STATx" |
| | ELAP_TM | DINT | Abgelaufene Zeit für Zeitverzögerung (DELAY_V) in ms |

## CONFIG_V

Die Informationen im Ausgangsparameter CONFIG_V des Cause-Meldebausteins F_SC_AL sind wie folgt hinterlegt:

| Bit Nr. | Belegung |
|---|---|
| Bit 0 | Auslösen bei "Bad Quality" |
| Bit 1 | - |
| Bit 2 | Soft-Bypass zulässig |
| Bit 3 | Automatisch quittierter aktiver Cause |
| Bit 4<br>Bit 5<br>Bit 6 | Funktionstyp:<br>1: Normal<br>2: 2oo3<br>3: UND<br>4: ODER<br>6: nur Kommentar |
| Bit 7 | Alarm bei Auslösung eines Inputs |
| Bit 8<br>Bit 9<br>Bit 10 | 0= Auslösung bei TAG = FALSE<br>1= Auslösung bei TAG = TRUE |
| Bit 11 | - |
| Bit 12 | Limit-Typ:<br>0= low<br>1= high |
| Bit 13 | - |
| Bit 14 | Gegenseitig verriegelte TAG-Simulation |
| Bit 15 | Cause genutzt |
| Bit 16 | Input-Typ: |

| Bit Nr. | Belegung |
|---|---|
| Bit 17 | 1= diskret<br>2= analog |
| Bit 18 | Anzahl der Inputs:<br>1= 1 Input<br>2= 2 Inputs<br>3= 3 Inputs |
| Bit 19 | |
| Bit 20 | |
| Bit 21 | Zeitverhalten:<br>0= keine Zeitbearbeitung<br>1= Einschaltverzögerung<br>2= Ausschaltverzögerung<br>3= Zeitgesteuerter Cause |
| Bit 22 | |
| Bit 23 | - |
| Bit 24 | First Out Alarm-Gruppe |
| Bit 25 | |
| Bit 26 | |
| Bit 27 | |
| Bit 28 | TAG1: externer Input |
| Bit 29 | TAG2: externer Input |
| Bit 30 | TAG3: externer Input |
| Bit 31 | - |

## STATE_V

Die Informationen im Ausgangsparameter STATE_V des Cause-Meldebausteins F_SC_AL sind wie folgt hinterlegt:

| Bit Nr. | Belegung |
|---|---|
| Bit 0 | Bypass aktiv (Bypass-TAG oder Soft-Bypass) |
| Bit 1 | Soft-Bypass aktiv |
| Bit 2 | Quittierung erfolgt |
| Bit 3 | Verknüpfungsergebnis der TAGs =1 |
| Bit 4 | Auslösung TAG1 |
| Bit 5 | Auslösung TAG2 |
| Bit 6 | Auslösung TAG3 |
| Bit 7 | - |
| Bit 8 | Cause aktiv |
| Bit 9 | Zeitbearbeitung aktiv |
| Bit 10 | Unterdrücken-TAG aktiv |
| Bit 11 | Hysterese aktiv |
| Bit 12 | TAG1: Simulation |
| Bit 13 | TAG2: Simulation |
| Bit 14 | TAG3: Simulation |
| Bit 15 | - |
| Bit 16 | - |
| Bit 17 | - |

| Bit Nr. | Belegung |
|---|---|
| Bit 18 | - |
| Bit 19 | - |
| Bit 20 | Positive Flanke an Bit 8 |
| Bit 21 | - |
| Bit 22 | - |
| Bit 23 | Cause genutzt |
| Bit 24 | - |
| Bit 25 | - |
| Bit 26 | - |
| Bit 27 | - |
| Bit 28 | Wert TAG1, der in der Safety Matrix bearbeitet wird |
| Bit 29 | Wert TAG2, der in der Safety Matrix bearbeitet wird |
| Bit 30 | Wert TAG3, der in der Safety Matrix bearbeitet wird |
| Bit 31 | - |

## DIAG_V

Die Informationen im Ausgangsparameter DIAG_V des Cause-Meldebausteins F_SC_AL sind wie folgt hinterlegt:

| Bit Nr. | Belegung |
|---|---|
| Bit 0 | - |
| Bit 1 | - |
| Bit 2 | - |
| Bit 3 | - |
| Bit 4 | Projektierte First Out Alarm-Gruppe |
| Bit 5 | |
| Bit 6 | |
| Bit 7 | |
| Bit 8 | PROFIsafe-Fehler Baugruppe TAG1 |
| Bit 9 | PROFIsafe-Fehler Baugruppe TAG2 |
| Bit 10 | PROFIsafe-Fehler Baugruppe TAG3 |
| Bit 11 | - |
| Bit 12 | Vorwarnung TAG1 |
| Bit 13 | Vorwarnung TAG2 |
| Bit 14 | Vorwarnung TAG3 |
| Bit 15 | - |
| Bit 16 | Fehlerhafte Konfiguration |
| Bit 17 | SDF-Fehler (Fehler im Sicherheitsdatenformat) |
| Bit 18 | Konfiguration verändert |
| Bit 19 | - |
| Bit 20 | Kanalfehler TAG1 |
| Bit 21 | Kanalfehler TAG2 |

| Bit Nr. | Belegung |
|---|---|
| Bit 22 | Kanalfehler TAG3 |
| Bit 23 | - |
| Bit 24 | Bad Quality TAG1 |
| Bit 25 | Bad Quality TAG2 |
| Bit 26 | Bad Quality TAG3 |
| Bit 27 | - |
| Bit 28 | Delta-Alarm TAG1 und 2 |
| Bit 29 | Delta-Alarm TAG2 und 3 |
| Bit 30 | Delta-Alarm TAG3 und 1 |
| Bit 31 | Auslösung eines TAG |

## CH_STATx

Die Informationen in den Ausgangsparametern CH_STAT1 bis 3 des Cause-Meldebausteins F_SC_AL sind wie folgt hinterlegt:

| Bit Nr. | Belegung |
|---|---|
| Bit 0 | QBAD |
| Bit 1 | QSIM (inaktiv) |
| Bit 2 | PASS_OUT (Fehler) |
| Bit 3 | ACK_REQ |
| Bit 4 | PASS_ON |
| Bit 5 | Redundante Baugruppe vorhanden |
| Bit 6 | PROFIsafe-Fehler |
| Bit 7 | PROFIsafe-Fehler redundante Baugruppe |
| Bit 8 | QCHF_LL (nur Analog-TAG) |
| Bit 9 | QCHF_HL (nur Analog-TAG) |
| Bit 10 | QSUBS |
| Bit 11 | - |
| Bit 12 | - |
| Bit 13 | - |
| Bit 14 | - |
| Bit 15 | - |

Weiterführende Informationen können dem entsprechenden F-Kanaltreiber entnommen werden.

## Siehe auch

Safety Matrix-Meldebaustein F_MA_AL (Seite 63)

Effect-Meldebaustein F_SE_AL (Seite 69)

### 4.1.6.4 Effect-Meldebaustein F_SE_AL

## Zusätzliche Informationen zur Weiterverarbeitung

An den Effect-Meldebausteinen F_SE_AL im *CFC* stehen Ihnen zusätzliche Informationen zur Weiterverarbeitung zur Verfügung. Ebenso können Sie Funktionen wie "Sperren der Alarme beim Hochlauf" im *CFC* projektieren.

## Anschlüsse des Effect-Meldebausteins F_SE_AL

| | Name | Datentyp | Erklärung |
|---|---|---|---|
| Eingänge: | M_Name | String[16] | Matrix-Name |
| | Number | INT | Effect-Nummer |
| | MSG_LOCK | BOOL | 1=Sperren aller Alarme |
| | | | |
| Ausgänge | CONFIG_V | DWORD | Effect-Konfiguration; siehe unten: Tabelle "CONFIG_V" |
| | STATE_V | DWORD | Effect-Status; siehe unten: Tabelle "STATE_V" |
| | DIAG_V | DWORD | Effect-Fehler; siehe unten: Tabelle "DIAG_V" |
| | OVERTM_W | DINT | Projektierte Warnzeit für Vorwarnung Übersteuern-Timeout in ms; bei Überschreitung dieses Wertes wird eine Warnung ausgegeben |
| | OVERTM_V | DINT | Projektierter Zeitwert für die maximale Zeit Übersteuern in ms |
| | DELAY_V | DINT | Projektierter Zeitwert für die Zeitbearbeitung zur Aktivierung des Effect in ms |
| | TAG1_B | BOOL | Wert TAG1, der in der Safety Matrix gebildet wird |
| | TAG2_B | BOOL | Wert TAG2, der in der Safety Matrix gebildet wird |
| | TAG3_B | BOOL | Wert TAG3, der in der Safety Matrix gebildet wird |
| | TAG4_B | BOOL | Wert TAG4, der in der Safety Matrix gebildet wird |
| | ACK_REQ | BOOL | 1= Quittierungsanforderung für Übersteuern-Fehler |
| | ACTIVE | BOOL | 1= Effect ist aktiviert<br>0= Effect ist nicht aktiviert |
| | ANY_BYP | BOOL | 1= wenn eine der folgenden Umgehungen aktiv ist:<br>(Hard-)Bypass, Soft-Bypass, Simulation eines TAG |
| | OK_RESET | BOOL | 1= Quittierungsanforderung für "Effect rücksetzen" |
| | OVER_AL | BOOL | 1= wenn die projektierte Warnzeit für Übersteuern-Timeout (OVERTM_W) überschritten wird |
| | ANY_DIAG | BOOL | 1= wenn Diagnosemeldungen vorliegen (DIAG_V nicht 0) |
| | CH_STAT1 | WORD | Wenn der TAG mit einem Kanaltreiber verbunden ist, wird hier der Kanalstatus angezeigt (TAG1); siehe unten: Tabelle "CH_STATx" |
| | CH_STAT2 | WORD | Wenn der TAG mit einem Kanaltreiber verbunden ist, wird hier der Kanalstatus angezeigt (TAG2); siehe unten: Tabelle "CH_STATx" |
| | CH_STAT3 | WORD | Wenn der TAG mit einem Kanaltreiber verbunden ist, wird hier der Kanalstatus angezeigt (TAG3); siehe unten: Tabelle "CH_STATx" |
| | CH_STAT4 | WORD | Wenn der TAG mit einem Kanaltreiber verbunden ist, wird hier der Kanalstatus angezeigt (TAG4); siehe unten: Tabelle "CH_STATx" |
| | ELAP_TM | DINT | Abgelaufene Zeit von DELAY_V bzw. OVERTM_V in ms (abhängig von der aktiven Funktion: Bit 9 aus Ausgangsparameter STATE_V = TRUE → DELAY_V; Bit 11 aus STATE_V = TRUE → OVERTM_V; siehe unten: Tabelle "STATE_V") |

## CONFIG_V

Die Informationen im Ausgangsparameter CONFIG_V des Effect-Meldebausteins F_SE_AL sind wie folgt hinterlegt:

| Bit Nr. | Belegung |
|---|---|
| Bit 0 | - |
| Bit 1 | Aktiviert "Prozesswert durchreichen" |
| Bit 2 | Soft-Bypass zulässig |
| Bit 3 | - |
| Bit 4 | Funktionstyp:<br>1: Normal<br>3: nur Kommentar |
| Bit 5 | |
| Bit 6 | |
| Bit 7 | - |
| Bit 8 | 0= Bei Effect aktiv TAG = FALSE<br>1= Bei Effect aktiv TAG = TRUE |
| Bit 9 | |
| Bit 10 | |
| Bit 11 | |
| Bit 12 | - |
| Bit 13 | Ausgabeverzögerung |
| Bit 14 | - |
| Bit 15 | 0= keine Auslösung Übersteuern-Timeout-Vorwarnung<br>1= Auslösung Übersteuern-Timeout-Vorwarnung |
| Bit 16 | - |
| Bit 17 | - |
| Bit 18 | - |
| Bit 19 | - |
| Bit 20 | - |
| Bit 21 | - |
| Bit 22 | Gegenseitig verriegelte TAG-Simulation |
| Bit 23 | Effect genutzt |
| Bit 24 | - |
| Bit 25 | - |
| Bit 26 | - |
| Bit 27 | - |
| Bit 28 | TAG1: externer Output |
| Bit 29 | TAG2: externer Output |
| Bit 30 | TAG3: externer Output |
| Bit 31 | TAG4: externer Output |

## STATE_V

Die Informationen im Ausgangsparameter STATE_V des Effect-Meldebausteins F_SE_AL sind wie folgt hinterlegt:

| Bit Nr. | Belegung |
|---|---|
| Bit 0 | Bypass aktiv (Bypass-TAG oder Soft-Bypass) |
| Bit 1 | Soft-Bypass aktiv |
| Bit 2 | "Prozesswert durchreichen" aktiv |
| Bit 3 | - |
| Bit 4 | Altwert Rücksetzen-/Übersteuern-TAG |
| Bit 5 | Übersteuern zulässig |
| Bit 6 | Quittierungsanforderung für Rücksetzen |
| Bit 7 | Effect verriegelt |
| Bit 8 | Effect aktiv |
| Bit 9 | Zeitbearbeitung aktiv |
| Bit 10 | Maskierungsfreigabe-TAG aktiv |
| Bit 11 | Übersteuern aktiv |
| Bit 12 | TAG1: Simulation |
| Bit 13 | TAG2: Simulation |
| Bit 14 | TAG3: Simulation |
| Bit 15 | TAG4: Simulation |
| Bit 16 | - |
| Bit 17 | - |
| Bit 18 | - |
| Bit 19 | - |
| Bit 20 | - |
| Bit 21 | - |
| Bit 22 | - |
| Bit 23 | Effect genutzt |
| Bit 24 | Effect nicht speichernd angefordert |
| Bit 25 | Effect speichernd angefordert |
| Bit 26 | Effect übersteuerbar angefordert |
| Bit 27 | Effect rücksetzbar und übersteuerbar angefordert |
| Bit 28 | Wert TAG1, der von der Safety Matrix gebildet wurde |
| Bit 29 | Wert TAG2, der von der Safety Matrix gebildet wurde |
| Bit 30 | Wert TAG3, der von der Safety Matrix gebildet wurde |
| Bit 31 | Wert TAG4, der von der Safety Matrix gebildet wurde |

## DIAG_V

Die Informationen im Ausgangsparameter DIAG_V des Effect-Meldebausteins F_SE_AL sind wie folgt hinterlegt:

| Bit Nr. | Belegung |
|---|---|
| Bit 0 | - |
| Bit 1 | - |
| Bit 2 | - |
| Bit 3 | - |
| Bit 4 | - |
| Bit 5 | - |
| Bit 6 | - |
| Bit 7 | - |
| Bit 8 | PROFIsafe-Fehler Baugruppe TAG1 |
| Bit 9 | PROFIsafe-Fehler Baugruppe TAG2 |
| Bit 10 | PROFIsafe-Fehler Baugruppe TAG3 |
| Bit 11 | PROFIsafe-Fehler Baugruppe TAG4 |
| Bit 12 | Vorwarnung Übersteuern-Timeout |
| Bit 13 | - |
| Bit 14 | - |
| Bit 15 | - |
| Bit 16 | - |
| Bit 17 | SDF-Fehler (Fehler im Sicherheitsdatenformat) |
| Bit 18 | - |
| Bit 19 | - |
| Bit 20 | Kanalfehler TAG1 |
| Bit 21 | Kanalfehler TAG2 |
| Bit 22 | Kanalfehler TAG3 |
| Bit 23 | Kanalfehler TAG4 |
| Bit 24 | Bad Quality TAG1 |
| Bit 25 | Bad Quality TAG2 |
| Bit 26 | Bad Quality TAG3 |
| Bit 27 | Bad Quality TAG4 |
| Bit 28 | Abbruch Übersteuern wegen neuer Cause-Auslösung |
| Bit 29 | Abbruch Übersteuern wegen Zeitüberschreitung |
| Bit 30 | - |
| Bit 31 | - |

## CH_STATx

Die Informationen in den Ausgangsparametern CH_STAT1 bis 3 des Effect-Meldebausteins F_SE_AL sind wie folgt hinterlegt:

| Bit Nr. | Belegung |
|---|---|
| Bit 0 | QBAD |
| Bit 1 | QSIM (inaktiv) |
| Bit 2 | PASS_OUT (Fehler) |
| Bit 3 | ACK_REQ |
| Bit 4 | PASS_ON |
| Bit 5 | Redundante Baugruppe vorhanden |
| Bit 6 | PROFIsafe-Fehler |
| Bit 7 | PROFIsafe-Fehler redundante Baugruppe |
| Bit 8 | QCHF_LL (nur Analog-TAG) |
| Bit 9 | QCHF_HL (nur Analog-TAG) |
| Bit 10 | QSUBS |
| Bit 11 | - |
| Bit 12 | - |
| Bit 13 | - |
| Bit 14 | - |
| Bit 15 | - |

Weiterführende Informationen können dem entsprechenden F-Kanaltreiber entnommen werden.

## Siehe auch

Safety Matrix-Meldebaustein F_MA_AL (Seite 63)

Cause-Meldebaustein F_SC_AL (Seite 64)

## 4.1.7 OS-Anbindung

### Voraussetzung für das Erzeugen von Bausteinsymbolen

Voraussetzung für das Erzeugen der Bausteinsymbole für die Safety Matrix ist die entsprechende Projektierung der Meldebausteine und der Transfer der Safety Matrix mit aktivierter Option "Alarm-Bausteine platzieren":

- im Dialog "Eigenschaften" der Safety Matrix, Register "Alarme"
  (siehe Kapitel "Der Dialog "Eigenschaften" der Safety Matrix (Seite 75)")
- im Dialog "Cause-Details", Register "Alarme"
  (siehe Kapitel "Dialog "Cause-Details" - Register "Alarme" (Seite 93)")
- im Dialog "Effect-Details ", Register "Alarme"
  (siehe Kapitel "Dialog "Effect-Details" - Register "Alarme" (Seite 101)")
- im Dialog "Transferieren ins Projekt", Register "Optionen"
  (siehe Kapitel "Transferieren der Safety Matrix in das Projekt (Seite 111)")

### Benutzerberechtigungen

Die Benutzerberechtigungen, z. B. für die Alarmquittierung in der PCS 7 OS, projektieren Sie im Dialog "Eigenschaften" der Safety Matrix, Register "Berechtigungen OS" (siehe Kapitel "Der Dialog "Eigenschaften" der Safety Matrix (Seite 75)").

Ab V6.2 gibt es an den Bausteinsymbolen der Safety Matrix eine Berechtigung für die Sammelquittierung von Alarmen und Meldungen (siehe Kapitel "Öffnen der Safety Matrix Viewer-Bildbausteine (Seite 127)").

# 4.2 Bearbeiten der Eigenschaften der Safety Matrix

## 4.2.1 Der Dialog "Eigenschaften" der Safety Matrix

### Der Dialog "Eigenschaften" der Safety Matrix

Wählen Sie den Menübefehl **Bearbeiten > Eigenschaften**. Der Dialog "Eigenschaften - (Matrixname)" wird mit dem Register "Allgemein" geöffnet.

### Register "Allgemein"

**Titel**

Geben Sie einen Titel zur Bezeichnung der Safety Matrix ein. Dieser wird im Informationsbereich der Safety Matrix-Eigenschaften angezeigt.

**Projekt**

Geben Sie ggf. den Namen des Projekts ein, zu dem die Safety Matrix gehört. Dieser wird im Informationsbereich der Safety Matrix-Eigenschaften angezeigt.

**Beschreibung**

Geben Sie eine prozessbezogene Beschreibung der Safety Matrix ein. Diese wird im Informationsbereich der Safety Matrix-Eigenschaften angezeigt.

**Allgemeine Kommentare**

Geben Sie allgemeine Anmerkungen zu dieser speziellen Safety Matrix ein.

**Kommentare**

Dies sind Anmerkungen, die im Informationsbereich für Kommentare rechts neben den Schnittpunkten angezeigt werden. Es können bis zu 32 Anmerkungen eingegeben werden, jede Anmerkung darf bis zu 63 Zeichen enthalten (Diese Anmerkungen können mit bestimmten Causes und/oder Effect verknüpft werden. Zu jedem Cause und Effect können in dem zugehörigen "Optionen"-Dialog maximal vier Anmerkungen eingegeben werden.)

**Sicherheitstechnische Funktionsgruppen**

Sicherheitstechnische Funktionsgruppen (Safety Instrumented Function groups, SIF) können Sie hier nach Maßgabe Ihrer Anwendung selbst anlegen, d. h. Sie unterteilen Ihre Anwendung in Funktionsgruppen, die Sie dann im *Safety Matrix Engineering Tool* und *Safety Matrix Viewer* gezielt beobachten und ändern können (z. B. "Füllstandsmessung und Abschaltung").

Um diese Funktion nutzen zu können, müssen Sie die einzelnen Causes und Effects des Sicherheitsprogramms Ihren Sicherheitstechnischen Funktionsgruppen zuordnen. Siehe dazu Kapitel "Dialog "Cause-Details" - Register "Optionen" (Seite 90)" bzw. "Dialog "Effect-Details" - Register "Optionen" (Seite 98)".

Nachdem Sie die Sicherheitstechnischen Funktionsgruppen im Dialog "Eigenschaften", Register "Allgemein" angelegt und bei den Optionen der Causes und Effects zugeordnet haben, können Sie einzelne, mehrere oder alle Sicherheitstechnischen Funktionsgruppen anzeigen. Dazu gehen Sie folgendermaßen vor:

- Klicken Sie auf die Schaltfläche "SIF" und wählen Sie die Sicherheitstechnische(n) Funktionsgruppe(n) aus, die Sie anzeigen möchten. Die Causes und Effects aller anderen Sicherheitstechnischen Funktionsgruppen werden ebenso ausgeblendet wie diejenigen Causes und Effects, die keiner Sicherheitstechnischen Funktionsgruppe zugeordnet sind.
  Oder:
- Wählen Sie den Menübefehl **Ansicht > Anpassen > Layout** und aktivieren Sie im Register "Allgemein" das Kontrollkästchen "Zeige First Out-/SIF-Gruppen". Bestätigen Sie mit "OK". Daraufhin wird in den "Causes"- und "Effects"-Tabellen die Spalte "Gruppen" eingeblendet, die anzeigt, welcher First Out (FO) Alarm-Gruppe und welchen Sicherheitstechnischen Funktionsgruppen die einzelnen Causes und Effects zugeordnet sind

#### Matrix-Zykluszeit (ms)

Damit kann die Zykluszeit der CPU, in die die Safety Matrix übertragen wird, festgelegt werden. In dem Dropdown-Menü kann die gewünschte Zeit aus den vorhandenen Auswahlmöglichkeiten (alle in ms) ausgewählt werden. Diese Zykluszeiten gehören zu den projektierten Ausführungszeiten von OB 30 bis 38.

### Register "Version"

#### Hauptversion

Anzeige der Nummer der Hauptversion. Mit der Schaltfläche "Nächste Version" können Sie die nächstfolgende Hauptversion anlegen. Sie werden aufgefordert, diese mit einer Beschreibung zu versehen. Automatisch wird jeder Hauptversion ein Zeitstempel hinzugefügt.

#### Nebenversion

Anzeige der Nummer der Nebenversion. Mit der Schaltfläche "Nächste Version" können Sie die nächstfolgende Nebenversion anlegen. Automatisch wird jeder Nebenversion ein Zeitstempel hinzugefügt. Beim Hochschalten der Nummer der Hauptversion wird die Nummer der Nebenversion auf Null zurückgesetzt. Jedes Mal, wenn Sie kritische Änderungen akzeptieren (siehe Kapitel "Der Menübefehl "Änderungsverfolgung" (Seite 82) "), wird die Nebenversion hochgezählt.

#### Dateiversion

Anzeige der Versionsnummer und des Zeitstempels der zuletzt gespeicherten Safety Matrix-Datei.

#### Safety Matrix-Signatur

Anzeige der aktuellen Signatur der Safety Matrix.

## Register "Datei"

### Safety Matrix-Dateiverzeichnis

Gibt den Dateipfad an, unter dem die Safety Matrix-Datei (.cem) gespeichert ist.

### SIMATIC-Projektverzeichnis

Gibt den Pfad zum SIMATIC-Projekt an, zu dem die Safety Matrix gehört. (Nur, wenn für die Safety Matrix ein Safety Matrix-Objekt im SIMATIC Manager existiert. Ansonsten ist dieses Feld leer.)

### Logischer Pfad zum S7-Programm

Gibt den Pfad zum S7-Programm, zu dem die Safety Matrix gehört, in der Komponentensicht an. (Nur, wenn für die Safety Matrix ein Safety Matrix-Objekt im SIMATIC Manager existiert. Ansonsten ist dieses Feld leer.)

### Safety Matrix in Technologischer Hierarchie

Gibt den Pfad zur Safety Matrix in der Technologischen Hierarchie an. (Nur, wenn für die Safety Matrix ein Safety Matrix-Objekt in der Technologischen Hierarchie existiert. Ansonsten ist dieses Feld leer.)

## Register "Statistik"

Enthält Angaben zur Nutzungsstatistik: Anzahl der Causes, der Effects und der Schnittpunkte.

## Register "Berechtigungen"

Enthält Angaben zu den Berechtigungen. Eventuell fehlende Berechtigungen werden hier angezeigt.

## Register "Parameter"

### Secure Write

Im Feld "Freigabe TAG" ist "#EN_SWC" fest eingestellt. Über diesen booleschen Eingang des hierarchischen Plans der Safety Matrix muss die Funktion Secure Write für das Bedienen im Online-Betrieb des Engineering Tools und von der PCS 7 OS mittels eines vor dem Übersetzen im *CFC* verdrahteten Signals freigegeben (= TRUE) und ggf. auch abgebrochen werden.

Im Feld "Zeitintervall"geben Sie die Zeit in Sekunden an, die bei der Secure Write-Transaktion als Timeout-Zeit verwendet wird.

---

**Hinweis**

Zum Bedienen der Safety Matrix mit dem *Safety Matrix Viewer* ist Secure Write erforderlich; ist Secure Write nicht freigegeben, so kann nur gelesen werden.

---

Siehe Kapitel "Secure Write (Seite 136)" und "Transferieren der Safety Matrix in das Projekt (Seite 111)".

## Register "Alarme"

### Alarm-Bausteine

Feld "Wiederholungszeit":
Hier können Sie die Zeit in Minuten für die zyklische Wiederholung von Bypass- und Unterdrückungsmeldungen angeben. Wenn die Meldung nach dieser Zeit immer noch ansteht, wird sie in einem Zyklus als gehend und dann wieder als kommend gemeldet. Die Voreinstellung für diese Zeit beträgt 8 Stunden. Wenn Sie die Zeit mit "0" parametrieren, erfolgt keine zyklische Wiederholung.

Kontrollkästchen "Platzieren für Cause und Effect":
Dieses Kontrollkästchen **müssen** Sie aktivieren, wenn Sie Meldungen **für einzelne Causes und Effects ermöglichen** möchten (Meldebausteine F_SC_AL und F_SE_AL). Diese Aktivierung ist die Voraussetzung dafür, dass in den Dialogen "Cause-Details" bzw. "Effect-Details" das Register "Alarme" erscheint, in dem Sie den Meldebaustein für den betreffenden Cause bzw. Effect platzieren und die Meldungen projektieren (siehe Kapitel "Dialog "Cause-Details" - Register "Alarme" (Seite 93)" bzw. "Dialog "Effect-Details" - Register "Alarme" (Seite 101)").

Kontrollkästchen "Platzieren für Matrix":
Dieses Kontrollkästchen **müssen** Sie aktivieren, wenn Sie Meldungen **für die Safety Matrix** ermöglichen möchten (Meldebaustein F_MA_AL). Weiter gehen Sie folgendermaßen vor:

- Ordnen Sie ggf. im Feld "Planzuordnung" den Meldebaustein für die Safety Matrix einer Technologischen Hierarchie zu. Mit Klick auf die zugehörige Schaltfläche "..." öffnet sich dafür ein Browser.
- Aktivieren Sie das Kontrollkästchen "Matrix-Meldungen freigeben", um diese Meldungen insgesamt freizugeben. Mit Klick auf die zugehörige Schaltfläche "..." öffnet sich der Dialog für die Projektierung des vordefinierten Alarm-Profils für die Safety Matrix. Dort können Sie
  - einzelne Meldungen freigeben
  - Meldeklassen ändern
  - Prioritäten der Meldeklassen ändern
  - die Quittieranforderung festlegen
- Aktivieren Sie das Kontrollkästchen "Sammelmeldungen freigeben". Dabei handelt es sich um die Verknüpfung der Zustände aller Meldebausteine von Causes und Effects. Mit Klick auf die zugehörige Schaltfläche "..." öffnet sich der Dialog für die Projektierung des vordefinierten Alarm-Profils für die Sammelmeldungen. Dort können Sie
  - Prioritäten der Meldeklassen ändern
  - die Quittieranforderung festlegen

## Register "Berechtigungen OS"

In diesem Register projektieren Sie die Benutzerberechtigungen, d. h. die Zuordnung der Funktionen der Safety Matrix zu einer Berechtigungsstufe in der PCS 7 OS.

Der *Safety Matrix Viewer* unterscheidet zwischen:

- **Beobachtungsfunktionen** ohne Zugriffschutz,
  d. h. ohne Zuordnung zu einer Berechtigungsstufe
- **Bedienfunktionen** mit Zugriffschutz,
  hierfür kann je Messstelle (Bausteinsymbol-Instanz) und je Bedienfunktion eine eigene Berechtigungsstufe festgelegt werden.
- **Bedienerrollen** mit Zugriffschutz,
  hierfür gibt es 2 Funktionen:
  - Initiator-Berechtigung: Der Bediener darf eine Bedienung **starten**.
  - Confirmer-Berechtigung: Der Bediener darf eine Bedienung **bestätigen**.

Siehe auch Kapitel "Initiator- und Confirmer-Berechtigung (Seite 134)".

Für alle Funktionen gilt: Berechtigungsstufe 0 bedeutet ‚kein Zugriffschutz', d. h. jeder Bediener hat diese Berechtigung.

Die Benutzer und eigene Berechtigungsstufen legen Sie in der PCS 7 OS mit dem Editor "User Administrator" an.

Die folgende Tabelle gibt einen Überblick über die Beobachtungs- und Bedienfunktionen und deren voreingestellte Berechtigungsstufen in der Safety Matrix.

| Funktion | Beschreibung | Default-Benutzerstufe |
|---|---|---|
| **Beobachtungsfunktionen** | | |
| Ereignisprotokoll anzeigen | | - |
| Cause-TAGs anzeigen | | - |
| Effect-TAGs anzeigen | | - |
| Cause Status anzeigen | | - |
| Effect Status anzeigen | | - |
| **Bedienerrollen** | | |
| Initiator | Berechtigungsstufe für Initiator | 0* |
| Confirmer | Berechtigungsstufe für Confirmer | 0* |
| **Bedienfunktionen** | | |
| Cause Quittierung | Berechtigungsstufe für Cause quittieren | 5 |
| Cause Bypass | Berechtigungsstufe für Cause Bypass | 5 |
| Cause-TAG Simulation An/Aus | Berechtigungsstufe für Cause-TAG simulieren | 5 |
| Cause-TAG Simulation Wert | Berechtigungsstufe für Cause-TAG Simulationswert festlegen | 5 |
| Cause First Out Alarm löschen | Berechtigungsstufe für Cause quittieren First Out | 5 |
| Effect Alarm löschen | Berechtigungsstufe für Übersteuern-Alarme löschen | 5 |
| Effect übersteuern | Berechtigungsstufe für Effect übersteuern | 5 |
| Effect rücksetzen | Berechtigungsstufe für Effect rücksetzen | 5 |
| Effect Bypass | Berechtigungsstufe für Effect Bypass | 6 |

| Funktion | Beschreibung | Default-Benutzerstufe |
|---|---|---|
| Effect-TAG Simulation An/Aus | Berechtigungsstufe für Effect-TAG simulieren | 6 |
| Effect-TAG Simulation Wert | Berechtigungsstufe für Effect-TAG Simulationswert festlegen | 6 |
| Ereignisse löschen | Berechtigungsstufe für Ereignisse löschen | 5 |
| Quittierung Treiber | Berechtigungsstufe für Kanaltreiber quittieren / reintegrieren | 5 |

*) Für die Initiator- und Confirmer-Berechtigung ist jeweils Berechtigungsstufe 0 (= Superuser) voreingestellt. Das 2-Bediener-Szenario wird aktiv, wenn unterschiedliche Berechtigungsstufen für Initiator und Confirmer eingetragen werden.

**Hinweis**

Die Berechtigungsstufe für die Sammelquittierung von Alarmen und Meldungen bearbeiten Sie direkt an den Bausteinsymbolen der Safety Matrix (siehe Kapitel "Öffnen der Safety Matrix Viewer-Bildbausteine (Seite 127)").

### 4.2.2 Die Dialoge "Anpassen"

#### Der Dialog "Anpassen - Layout"

#### Register "Allgemein"

Wählen Sie den Menübefehl **Ansicht > Anpassen > Layout**. Öffnen Sie das Register "Allgemein".

Wenn Sie die in diesem Register angebotenen Kontrollkästchen aktivieren, werden die für Causes (C) oder Effects (E) in der Safety Matrix vorgenommenen Einstellungen in zusätzlich eingeblendeten Spalten in den "Causes"- und "Effects"-Tabellen angezeigt.

**Zeige C/E Optionen**

Zeigt die für Causes (C) oder Effects (E) eingestellten Optionen an. Die folgende Liste erläutert die Abkürzungen, die in den zusätzlichen Anzeigespalten stehen können. Diese Liste wird auch im Informationsbereich unter den Schnittpunkten in der Safety Matrix angezeigt.

D - Verzögerung (Delay) konfiguriert

I - Unterdrückung (Inhibit) konfiguriert

M - Maskierung konfiguriert

B - Soft-Bypass zulässig

H - Hard-Bypass konfiguriert

N - Unechter (Non-physical) I/O-TAG konfiguriert (TAG mit Präfix "#")

P - Durchreichen des Prozesswerts konfiguriert

A - Automatische Quittierung von aktivem Cause konfiguriert

T - Zeitgesteuerter (Timed) Cause konfiguriert

**Zeige C/E Kommentare**

Zeigt die Nummer(n) der Kommentare, die diesem Cause bzw. Effect zugeordnet sind. Die den Nummern entsprechenden Anmerkungen werden im Informationsbereich "Kommentare" rechts neben den Schnittpunkten angezeigt.

**Zeige C/E SIL**

Zeigt die SIL-Nummer (Safety Integrity Level), die diesem Cause bzw. Effect zugeordnet ist.

**Zeige First Out-/SIF-Gruppen**

Zeigt die First Out- und/oder Sicherheitstechnischen Funktionsgruppen (SIF) an, denen dieser Cause bzw. Effect zugeordnet ist. Die First Out-Gruppe ist mit der Abkürzung "FO" gekennzeichnet. FO2 zeigt zum Beispiel an, dass der Cause zur First-Out-Gruppe (FO) 2 gehört. Die Nummern der Sicherheitsgruppen erscheinen hinter der First Out-Gruppennummer. Beispiel: FO3, 5, 17, 44 zeigt an, dass dieser Cause zur First Out-Gruppe (FO) 3 und den Sicherheitstechnischen Funktionsgruppen 5, 17 und 44 gehört.

**Zeige Rücksetzen-/Übersteuern-TAG**

Zeigt den Rücksetzen-/Übersteuern-TAG an, der dem Effect zugeordnet ist.

**Zeige I/O physikalische Adresse in Anzeige-TAGs**

Zeigt im Online-Betrieb nach Anklicken der Steuerleisten-Schaltfläche "Anzeige TAGs" die physikalische I/O-Adresse zusammen mit dem Symbol im Dialog "Anzeige TAGs - Cause x" an.

**Markiere Leisten-/Schnittpunkt-ToolTip**

Wenn Sie einen Schnittpunkt anklicken, wird die entsprechende Zeile und Spalte farblich hervorgehoben, und in einem ToolTip angezeigt, welcher Cause und welcher Effect damit verbunden werden.

**Markiere Dynamische Werte**

Hebt die dynamischen Werte in der F-CPU hervor. Diese werden an der Oberfläche im Unterschied zu parametrierten Werten in blauer Schrift dargestellt.

## Register "Größe"

Wählen Sie den Menübefehl **Ansicht > Anpassen > Layout**. Öffnen Sie das Register "Größe".

Wenn die Safety Matrix keine leeren Zeilen (für Causes) bzw. Spalten (für Effects) mehr enthält, so können Sie in diesem Dialog die Anzahl der Zeilen/Spalten vergrößern.

**Anzahl der Causes / Anzahl der Effects**

Standardmäßig sind hier 16 Causes/Effects eingetragen, diese Zahl kann bis auf 128 erhöht werden.

---

**Hinweis**

Wenn die Größe der Safety Matrix geändert wurde, aktiviert das *Safety Matrix Engineering Tool* beim Transfer der Safety Matrix automatisch die Transfer-Option "Plan + Parameter". Beachten Sie dazu Kapitel "Transferieren der Safety Matrix in das Projekt (Seite 111) ".

---

### Der Dialog "Anpassen - Farben"

### Register "Allgemein"

Wählen Sie den Menübefehl **Ansicht > Anpassen > Farben**. Öffnen Sie das Register "Allgemein".

Im Online-Betrieb der Safety Matrix wird der Status der Causes, Effects und Schnittpunkte mit verschiedenen Farben hinterlegt, deren Zuordnung in diesem Dialog angezeigt wird.

Die Zuordnung von Status bzw. Alarm-Profil zu Farbe und die Farbe des Textes können Sie ändern.

In der Voreinstellung werden vorgenommene Änderungen bzw. Unterschiede im Offline-Betrieb durch roten Text markiert. Dynamische Werte werden in blauer Schrift dargestellt, falls das Kontrollkästchen "Markiere Dynamische Werte" im Dialog "Anpassen - Layout", Register "Allgemein" aktiviert ist. Auch diese Zuordnung der Schriftfarben können Sie ändern.

Mit der Schaltfläche "PCS 7" können Sie die Farben der Safety Matrix an die *PCS 7*-Farbkonventionen anlehnen.

Mit der Schaltfläche "Rücksetzen" können Sie wieder die Voreinstellung der Safety Matrix aktivieren.




**Zuordnung der Farben**

Die Zuordnung der Farben muss allen relevanten anwendungsspezifischen Normen entsprechen und nach Maßgabe Ihrer Anwendung sinnvoll sein.

## 4.2.3 Der Menübefehl "Änderungsverfolgung"

### Handhabung von Änderungen

Sie können festlegen, wie die Safety Matrix Änderungen handhabt.

Wählen Sie den Menübefehl **Extras > Änderungsverfolgung > Änderungen akzeptieren**. Der Dialog "Nachverfolgte Änderungen - (Matrixname)" wird geöffnet.

Legen Sie fest, welche Art von Änderungen Sie akzeptieren wollen:

- Kritische Änderungen - dies sind ablaufrelevante Änderungen, z. B. bei der Anzahl von Zeilen oder Spalten der Safety Matrix
- Unkritische Änderungen - dies sind formale Änderungen, z. B. bei Kommentaren oder Anzeigefunktionen

Zur Unterstützung wird Ihnen die Möglichkeit geboten, das Protokoll zu überprüfen. Klicken Sie dazu auf die Schaltfläche **Zeige Details**.

### Speichern von Änderungen

Sie können festlegen, wie Änderungen in der Safety Matrix beim Speichern bzw. beim Speichern-als gehandhabt werden.

Wählen Sie dazu den Menübefehl **Extras > Änderungsverfolgung > Änderungen automatisch akzeptieren beim Speichern** bzw. **Änderungen automatisch akzeptieren beim Speichern-als**.

## 4.3 Projektieren der Causes

### 4.3.1 Übersicht zum Projektieren der Causes

#### Einleitung

Als Input-Typ stehen analoge und diskrete Werte zur Verfügung. Minimal ein Wert und maximal drei Werte bilden zusammen über den Funktionstyp einen Cause.

#### Diskrete Input-TAGs

Für jeden diskreten Input-TAG eines Cause kann entweder

- Energize-to-trip (ETT; Auslösen bei TRUE) oder
- Deenergize-to-trip (DTT; Auslösen bei FALSE) gewählt werden.

In der folgenden Tabelle wird davon ausgegangen, dass immer DTT eingestellt ist. Somit wird der Input-TAG aktiv, wenn er FALSE ist. Zusätzlich können die Input-TAGs auf ihre Qualität geprüft werden und bei mangelnder Qualität wird der Cause aktiv (Trip).

**Analoge Input-TAGs**

Bei den analogen Werten hängt die Aktivierung von einem Limit ab. Wurde dieses unter- oder überschritten, wird der Cause aktiv. Werden mehrere analoge Input-TAGs für einen Cause verwendet, wird eine vom Anwender angegebene zulässige Diskrepanz (Delta) ausgewertet. Unterscheiden sich die Werte um mehr als diese zulässige Diskrepanz, wird ein Diskrepanz-Alarm ausgelöst. Zusätzlich können die Input-TAGs auf ihre Qualität geprüft werden und bei mangelnder Qualität wird der Cause aktiv (Trip).

Tabelle 4- 1 Abhängigkeiten der Cause-Parameter untereinander

| Input-Typ | Anzahl der Inputs | Funktionstyp | Limit-Typ High / Low | Cause wird aktiv, wenn… |
|---|---|---|---|---|
| Diskret* | 1 | Normal | - | Input-TAG = FALSE |
| | | Nur Kommentar | - | Nie |
| | 2 | UND | - | beide Input-TAGs = FALSE |
| | | ODER | - | einer der beiden Input-TAGs = FALSE |
| | | Nur Kommentar | - | Nie |
| | 3 | 2oo3 | - | mindestens zwei von drei Input-TAGs = FALSE |
| | | UND | | alle drei Input-TAGs = FALSE |
| | | ODER | - | einer der drei Input-TAGs = FALSE |
| | | Nur Kommentar | - | Nie |

| Input-Typ | Anzahl der Inputs | Funktionstyp | Limit-Typ High / Low | Cause wird aktiv, wenn… |
|---|---|---|---|---|
| Analog | 1 | Normal | High | …der Input-TAG das Limit überschritten hat. Der Cause wird erst wieder inaktiv, wenn der Input-TAG das Limit abzüglich Hysterese unterschritten hat. |
| | | | Low | …der Input-TAG das Limit unterschritten hat. Der Cause wird erst wieder inaktiv, wenn der Input-TAG das Limit zuzüglich Hysterese überschritten hat. |
| | | Nur Kommentar | - | Nie |
| | 2 | UND | High | …beide Input-TAGs das Limit überschritten haben. Der Cause wird erst wieder inaktiv, wenn einer der beiden Input-TAGs das Limit abzüglich Hysterese unterschritten hat. |
| | | | Low | …beide Input-TAGs das Limit unterschritten haben. Der Cause wird erst wieder inaktiv, wenn einer der beiden Input-TAGs das Limit zuzüglich Hysterese überschritten hat. |
| | | ODER | High | …einer der zwei Input-TAGs das Limit überschritten hat. Der Cause wird erst wieder inaktiv, wenn beide Input-TAGs das Limit abzüglich Hysterese unterschritten haben. |
| | | | Low | …einer der beiden Input-TAGs das Limit unterschritten hat. Der Cause wird erst wieder inaktiv, wenn beide Input-TAGs das Limit zuzüglich Hysterese überschritten haben. |
| | | Nur Kommentar | - | Nie |
| | 3 | 2oo3 | High | …mindestens zwei der drei Input-TAGs das Limit überschritten haben. Der Cause wird erst wieder inaktiv, wenn mindestens zwei Input-TAGs das Limit abzüglich Hysterese unterschritten haben. |
| | | | Low | … mindestens zwei der drei Input-TAGs das Limit unterschritten haben. Der Cause wird erst wieder inaktiv, wenn mindestens zwei Input-TAGs das Limit zuzüglich Hysterese überschritten haben. |
| | | UND | High | …alle drei Input-TAGs das Limit überschritten haben. Der Cause wird erst wieder inaktiv, wenn einer der drei Input-TAGs das Limit abzüglich Hysterese unterschritten hat. |
| | | | Low | …alle drei Input-TAGs das Limit unterschritten haben. Der Cause wird erst wieder inaktiv, wenn einer der drei Input-TAGs das Limit zuzüglich Hysterese überschritten hat. |
| | | ODER | High | …einer der drei Input-TAGs das Limit überschritten hat. Der Cause wird erst wieder inaktiv, wenn alle drei Input-TAGs das Limit abzüglich Hysterese unterschritten haben. |
| | | | Low | …einer der drei Input-TAGs das Limit unterschritten hat. Der Cause wird erst wieder inaktiv, wenn alle drei Input-TAGs das Limit zuzüglich Hysterese überschritten haben. |
| | | Nur Kommentar | - | Nie |

* wenn DTT für alle TAGs des Cause projektiert ist

### 4.3.2 Cause und Zeile für Cause anlegen/ändern

#### Vorgehensweise zum Anlegen/Ändern eines Cause

Doppelklicken Sie im Konfigurationsbereich Causes der Safety Matrix auf eine (leere oder befüllte) Zeile oder klicken Sie auf die Zeile und wählen Sie "Ändern Cause" im Kontextmenü.
Der Dialog "Cause-Details - Cause x" wird geöffnet und Sie können den Cause anlegen oder ändern.

#### Das Kontextmenü im Konfigurationsbereich Causes der Safety Matrix

Wenn Sie im Konfigurationsbereich Causes der Safety Matrix auf eine Zeile klicken, so stellt Ihnen das Kontextmenü, je nach leerer oder bereits befüllter Zeile, die folgenden Funktionen zur Verfügung:

**Bei leerer Zeile:**

- Ändern Cause (der Dialog "Cause-Details - Cause x" wird geöffnet)
- Einfügen Zeile
- Löschen Zeile

**Bei befüllter Zeile:**

- Kopieren Cause
- Ausschneiden Cause
- Ändern Cause (der Dialog "Cause-Details - Cause x" wird geöffnet)
- Löschen Cause (der Cause, d. h. der Inhalt der Zeile wird gelöscht, aber die Zeile bleibt als leere Zeile erhalten)
- Einfügen Zeile (eine leere Zeile wird eingefügt und alle nachfolgenden Causes werden um eine Zeile nach unten verschoben)
- Löschen Zeile (die aktuelle Zeile wird gelöscht, und alle nachfolgenden Causes werden um eine Zeile nach oben verschoben)

---

**Hinweis**

Bei "Einfügen Zeile" wird die letzte Zeile der Safety Matrix immer gelöscht. Stellen Sie deshalb sicher, dass die letzte Zeile leer ist. Gegebenenfalls müssen Sie die Größe der Safety Matrix anpassen.

---

**Hinweis**

Bei "Einfügen Zeile" bzw. "Löschen Zeile" aktiviert das *Safety Matrix Engineering Tool* beim Transfer der Safety Matrix automatisch die Transfer-Option "Plan + Parameter". Beachten Sie dazu Kapitel "Transferieren der Safety Matrix in das Projekt (Seite 111)".

---

**Hinweis**

"Einfügen Zeile" bzw. "Löschen Zeile" kann dazu führen, dass in einem anschließenden Matrix-Vergleich alle nachfolgenden Zeilen als geändert gekennzeichnet werden und somit bei einer Abnahme geprüft werden müssen. Sie können dies umgehen, indem Sie:

- zusätzliche Causes immer am Ende hinzufügen
- nicht ganze Zeilen ausschneiden, einfügen, kopieren, löschen, sondern nur deren Inhalte
- die Änderung der Größe der Safety Matrix vermeiden.

---

### 4.3.3 Übersicht über den Dialog "Cause-Details - Cause x"

#### Vorgehensweise zum Projektieren eines Cause

Doppelklicken Sie im Causes-Konfigurationsbereich der Safety Matrix auf eine (leere oder befüllte) Zeile oder klicken Sie auf die Zeile und wählen Sie "Ändern" im Kontextmenü.
Der Dialog "Cause-Details - Cause x" wird geöffnet.

**Cause "x"**

Jedem Cause ist eine eindeutige Nummer innerhalb der Safety Matrix zugeordnet. Die Zuordnung erfolgt automatisch auf Grund der ausgewählten Zeile. Die Cause-Nummer kann nicht geändert werden.

#### Dialog zum Projektieren eines Cause

Der Dialog zum Projektieren eines Cause besteht aus den Registern:

- "Konfigurieren"
- "Optionen"
- "Alarme"

Falls Sie im Register "Konfigurieren" als Input-Typ "Analog" auswählen, so wird noch ein weiteres Register eingefügt:

- "Analog-Parameter"

### 4.3.4 Dialog "Cause-Details" - Register "Konfigurieren"

#### Register "Konfigurieren"

| Feld | Beschreibung |
|---|---|
| Beschr. | Alphanumerische Beschreibung des Cause. Die Eingabe einer Beschreibung ist obligatorisch, sie kann bis zu 32 Zeichen lang sein. |
| SIL (= Safety Integrity Level) | Dieses Feld dient zu Dokumentationszwecken. Hier können Sie den SIL für diesen Cause eintragen, den Sie in der Risikoanalyse (z. B. nach IEC 61508) ermittelt haben.<br>Eine Eingabe in diesem Feld ist nicht erforderlich. In der Voreinstellung ist kein SIL-Wert eingegeben. |
| TAG x | Geben Sie für jeden Cause mindestens einen TAG an. Beachten Sie dazu das Kapitel "Syntaxregeln für TAG-Namen in der Safety Matrix (Seite 55)". |
| • (Schaltfläche) I/O | Mit Klick auf Schaltfläche "I/O" wird der Dialog "Auswahl I/O-TAG" geöffnet. Siehe Kapitel "Die TAGs der Safety Matrix (Seite 53)". |
| • (Schaltfläche) ... | Die Schaltfläche "..." erscheint, falls im Dialog "Auswahl I/O-TAG" die Option "Kanaltreiber" ausgewählt wurde. Mit Klick auf Schaltfläche "..." wird der Dialog "Kanaltreiber" geöffnet.<br>• Im Register "Parameter" können Sie für F-Kanaltreiber, die über Symbol ausgewählt werden:<br>– für analoge Input-TAGs die oberen und unteren Bereichsgrenzen für die Geber anzeigen und bearbeiten<br>• Im Register "Optionen" können Sie<br>– eine Vorverarbeitung für diesen Input-TAG durch Auswahl eines entsprechenden Vorverarbeitungs-Plans aktivieren bzw. die Vorverarbeitung abwählen. Siehe Kapitel "Die TAGs der Safety Matrix (Seite 53)".<br>– auswählen, ob Sie einen Startwert für die Simulation vorgeben möchten<br>– ggf. einen Startwert für die Simulation dieses Input-TAG vorgeben.<br>Diese Parameter können auch direkt an den F-Kanaltreibern in den *CFC*-Plänen bearbeitet werden (inkl. Verschalten). Wenn Sie diese Möglichkeit nutzen, müssen Sie beachten, dass es dadurch zu Überschneidungen kommen kann. Die Daten, die in *CFC* gespeichert sind, haben Vorrang.<br>Bereichsgrenzen können im Safety Matrix Editor nur angezeigt werden. |
| Input-Typ | Es muss zu jedem Cause ein Input-Typ gewählt werden. |
| • Diskret | Der diskrete Typ ist ein boolescher Wert (TRUE/FALSE). Er wird beispielsweise für Endschalter oder Motorkontrollsignale benutzt. Diskret ist die Standardeinstellung für den Input-Typ. |
| • Analog | Ein analoger Eingang stellt einen realen Wert dar, z. B. den Wert eines Temperaturgebers oder eine Durchflussmenge. Wird analog als Input-Typ gewählt, so müssen weitere Parameter eingestellt werden. Die Parametereinstellung erfolgt im Register "Analog-Parameter" des Dialogs "Cause-Details". |

| Feld | Beschreibung |
|---|---|
| Energize-to-trip | Dies ist eine Option für diskrete Input-Typen und legt fest, welcher boolesche Zustand eine Auslösung darstellt. In Deenergize-to-trip-Anwendungen stellt der Input-TAG eine Auslösung dar, wenn er nach OFF (FALSE) wechselt. In Energize-to-trip-Anwendungen stellt der Input-TAG eine Auslösung dar, wenn er nach ON (TRUE) wechselt. Standardmäßig ist dieses Kontrollkästchen nicht aktiviert, d. h. die Voreinstellung ist Deenergize-to-trip, da der Wert "0" bei digitaler F-Peripherie als sichere Ruhelage gilt. Siehe folgende Tabelle. |
| Anzahl der Inputs | Geben Sie an, wie viele TAGs einem bestimmten Cause zugeordnet sind. Werden beispielsweise drei Geber für die Überwachung ein- und desselben Prozesspunktes benutzt, so ist der Wert "3" auszuwählen. |
| Funktionstyp | Mit dem "Funktionstyp" bestimmen Sie, unter welchen Bedingungen ein Cause aktiv wird. Die Eingabe in diesem Feld ist obligatorisch.<br>Hinweis: Der Funktionstyp führt zu einem Auslösebefehl, der durch weitere Einstellungen im Register "Optionen" des Dialogs "Cause-Details" beeinflusst werden kann. |
| Alarm-Profil | Jedem Cause ist ein Alarm-Profil zugeordnet. Sie können die Alarm-Profile für die Causes und Effects projektieren (siehe Kapitel "Dialog "Cause-Details" - Register "Alarme" (Seite 93)").<br>Die Wahl des Alarm-Profils entscheidet über die Farbdarstellung im Online-Betrieb und ggf. über die abgesetzten Meldungen des Cause. |
| • Standard | Alarm-Profil "Standard" wird eingestellt (Voreinstellung). |
| • Sequential | Alarm-Profil "Sequential" wird eingestellt. |
| • Energized | Alarm-Profil "Energized" wird eingestellt. |

| Projektierung | Input-TAG | Cause* |
|---|---|---|
| DTT | 0 | aktiv |
| | 1 | inaktiv |
| ETT | 1 | aktiv |
| | 0 | inaktiv |

* abhängig vom projektierten Funktionstyp und den Optionen Bypass, Unterdrücken und Zeitverhalten

Beachten Sie hierzu auch Kapitel "Übersicht zum Projektieren der Causes (Seite 83)".

### 4.3.5 Dialog "Cause-Details" - Register "Analog-Parameter"

#### Register "Analog-Parameter"

| Feld | Beschreibung |
|---|---|
| Limit | Der in diesem Feld eingegebene Wert bedeutet, dass der Cause-TAG die Auslösebedingung erfüllt, wenn der TAG-Wert kleiner/gleich oder größer/gleich diesem Eingabewert - je nach dem ausgewählten Limit-Typ - ist. |
| Typ(en) | Diese Einstellung legt fest, ob das Limit ein oberer oder ein unterer Grenzwert ist. Ist es ein oberer Grenzwert, so erfüllt der Cause-TAG die Auslösebedingung, wenn sein Wert größer oder gleich dem Eingabewert im Feld "Limit" ist. Ist es ein unterer Grenzwert, so erfüllt der Cause-TAG die Auslösebedingung, wenn sein Wert kleiner oder gleich dem Eingabewert im Feld "Limit" ist. |
| Limit-Vorwarnung | Ein Cause-TAG wird in der für "Vorwarnung" projektierten Farbe hinterlegt, sobald der TAG-Wert kleiner/gleich oder größer/gleich diesem Eingabewert ist - je nach dem ausgewählten Limit-Typ.<br>Zur Deaktivierung dieser Option setzen Sie den Wert größer/gleich dem Limit-Wert. |
| Hysterese | Die Hysterese legt eine Totzone im Bereich des Grenzwertes fest, wenn ein Cause-TAG die Auslösebedingung nicht mehr erfüllt. So wird verhindert, dass ein Eingang ständig zwischen aktiv und inaktiv pendelt. In der Standardeinstellung ist keine Hysterese eingestellt, das entspricht einem Wert "0".<br>Beispiele:<br>Ist für den Cause ein "high limit" von 90,0 und eine Hysterese von 5,0 eingestellt, so bleibt der Cause aktiv, bis der Wert unter 85,0 fällt.<br>Ist für den Cause ein "low limit" von 10,0 und eine Hysterese von 2,0 eingestellt, so bleibt der Cause aktiv, bis der Wert über 12,0 steigt. |
| Diskrepanz | Dieses Feld erscheint nur bei analogen Eingängen mit mehr als einem Input-TAG. Es wird ein Diagnosealarm ausgelöst, wenn die Input-TAGs sich mindestens um den eingegebenen Diskrepanzwert unterscheiden. Zum Löschen eines Diagnosealarms müssen diese Werte innerhalb des Diskrepanzbereichs minus der Hysterese liegen.<br>Wird für "Diskrepanz" nichts oder ein Wert "0" eingegeben, so erfolgt keine Diskrepanzbetrachtung.<br>Beispiel: Ist ein Diskrepanzwert von 5,0 und eine Hysterese von 2,0 eingestellt, so wird ein Diagnosealarm angezeigt, wenn die Werte sich um 5,0 oder mehr unterscheiden. Die Werte müssen in einem Bereich von 3,0 liegen, damit der Diagnosealarm gelöscht wird. |
| Messeinheit | Gibt die Messeinheit des Analogwertes an. Diese Angabe kann bis zu 16 Zeichen lang sein und dient lediglich zu Dokumentationszwecken. |

Beachten Sie hierzu auch Kapitel "Übersicht zum Projektieren der Causes (Seite 83) ".

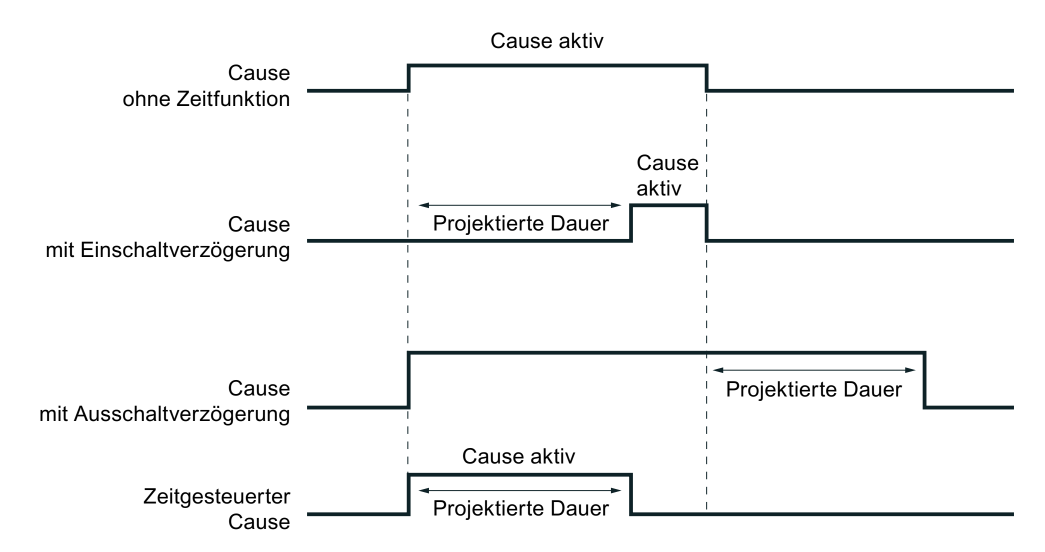
## 4.3.6 Dialog "Cause-Details" - Register "Optionen"

### Register "Optionen"

| Feld | Beschreibung |
|---|---|
| Zeitverhalten | Die Causes können so konfiguriert werden, dass die nachstehend beschriebenen Zeitfunktionen berücksichtigt werden. Siehe auch das Zeitablaufdiagramm für Cause-Zeitfunktionen im Anschluss an diese Tabelle. |
| • Keine | Mit diesem Kontrollkästchen werden alle Zeitoptionen zu diesem Cause gelöscht. "Keine" ist die Standardeinstellung. |
| • Einschaltver-zögerung | Damit wird eine Einschaltverzögerung eingestellt. Die Auslösebedingung für den Cause muss mindestens für die eingestellte Zeitdauer erfüllt sein, bevor der Cause aktiv wird. |
| • Ausschaltver-zögerung | Damit wird eine Ausschaltverzögerung eingestellt. Die Auslösebedingung für den Cause muss eine gewisse Zeit nicht erfüllt sein, bevor der Cause inaktiv wird. |
| • Zeitgesteuerter Cause | Ist zu einem Cause diese Option gewählt, so bleibt der Cause während der im Feld "Zeitdauer" eingegebenen Zeit aktiv, unabhängig davon, ob die Auslösebedingung des Cause die ganze Zeit TRUE bleibt oder nicht. |
| • Dauer | Hier geben Sie die gewünschte Zeitdauer für die Einstellungen **Einschaltverzögerung**, **Ausschaltverzögerung** oder **Zeitgesteuerter Cause** ein. |
| Bypass | Die Causes können so konfiguriert werden, dass die folgenden Umgehungsfunktionen (Bypass) möglich sind: |
| • Soft-Bypass zulässig | Ist das Kontrollkästchen "Soft-Bypass zulässig" aktiviert, so kann der Bediener im Viewer oder im Online-Betrieb des Engineering Tools manuell einen Bypass für Wartungszwecke anlegen. In der Voreinstellung ist dieses Kontrollkästchen aktiviert. |
| • Bypass-TAG | Mit Klick auf Schaltfläche "I/O" wird der Dialog "Auswahl I/O-TAG" geöffnet. Hier können Sie einen booleschen TAG als Bypass-TAG auswählen. Siehe Kapitel "Die TAGs der Safety Matrix (Seite 53)".<br>Für den Cause wird ein Bypass aktiv, wenn der Wert des Bypass-TAG TRUE ist. Ein Bypass wird in der Regel für Wartungszwecke angelegt. Bei aktivem Bypass wird der Cause nicht aktiv, obwohl er aufgrund seiner Auslösebedingung und Optionen aktiv sein sollte. |
| Unterdrücken-TAG | Mit Klick auf Schaltfläche "I/O" wird der Dialog "Auswahl I/O-TAG" geöffnet. Hier können Sie einen booleschen TAG als Unterdrücken-TAG auswählen. Siehe Kapitel "Die TAGs der Safety Matrix (Seite 53)".<br>Die Funktion Unterdrückung (Inhibit) wird typischerweise benutzt, um einen Cause während des automatischen Anfahrens in einem Batch-Prozess automatisch zu unterdrücken.<br>Der "Unterdrücken-TAG" ist ein boolescher TAG. Der Cause wird unterdrückt, wenn der Unterdrücken-TAG TRUE ist. Bei aktiver Unterdrückung wird der Cause nicht aktiv, obwohl er aufgrund seiner Auslösebedingung und Optionen aktiv sein sollte. |

<table>
<tr><th>Feld</th><th>Beschreibung</th></tr>
<tr><td>First Out Alarm-Gruppe</td><td>Im Online-Betrieb zeigt die First Out Alarm-Funktion an, welcher Cause zuerst aktiv geworden ist (d. h. die Auslösung veranlasst hat). Der Cause, der in jeder Gruppe zuerst ausgelöst hat, wird farblich hervorgehoben dargestellt. Ein Cause kann in jede beliebige der 15 verschiedenen First Out Alarm-Gruppen eingeordnet werden. Die First Out Alarm-Funktion ist in der Voreinstellung ausgeschaltet. Um einen Cause zu einer First Out Alarm-Gruppe hinzuzufügen, geben Sie einfach die Gruppennummer in diesem Textfeld ein.</td></tr>
<tr><td>Kommentare</td><td>Es können zu jeder Safety Matrix 32 Anmerkungen eingegeben werden, die im Informationsbereich für Kommentare angezeigt werden. In den Feldern "Kommentare" können jedem Cause bis zu vier Anmerkungen zugeordnet werden. Die Zahl im Kästchen neben jedem Feld bezieht sich auf die zugehörige Anmerkung.</td></tr>
<tr><td>Safety Instrumented Function (SIF) Gruppen</td><td>Ein Cause kann bis zu vier SIF-Gruppen, das sind "Sicherheitstechnische Funktionsgruppen (Safety Instrumented Function groups)", zugeordnet werden. Eine SIF-Gruppe enthält zusammengehörige Causes und Effects, die typischerweise einer einzigen Sicherheitsschaltung aus Gebern, F-CPU und den Steuerungselementen, die eine bestimmte Sicherheitsfunktion ausführen, zugeordnet sind. Mit der Zuordnung zu einer SIF-Gruppe können Filterfunktionen für die Anzeige im Online-Betrieb für Causes und Effects realisiert werden.<br><br>Sie müssen die Sicherheitstechnischen Funktionsgruppen im Dialog "Eigenschaften" der Safety Matrix, Register "Allgemein" angelegt haben, bevor Sie sie hier zuordnen können. Bitte beachten Sie die Ausführungen dazu im Kapitel "Der Dialog "Eigenschaften" der Safety Matrix (Seite 75) ".</td></tr>
<tr><td>Automatisch quittierter aktiver Cause</td><td>Ist das Kontrollkästchen "Automatisch quittierter aktiver Cause" aktiviert, so wird der Cause automatisch gelöscht, sobald die Auslösebedingung nicht mehr erfüllt ist. Ist dieses Kontrollkästchen nicht aktiviert, so muss der Bediener das Löschen eines aktiven Cause manuell veranlassen. In der Voreinstellung ist dieses Kontrollkästchen aktiviert.<br><br>Hinweis: Die Quittierung hat keine Auswirkung auf einen Cause mit projektierter Ausschaltverzögerung bzw. einen zeitgesteuerten Cause.</td></tr>
<tr><td>Auslösen bei "Bad Quality"</td><td>Ist das Kontrollkästchen "Auslösen bei "Bad Quality"" aktiviert, so bewirken die von den F-Kanaltreibern gemeldeten Qualitätsfehler, dass der Input-TAG zwangsweise den ausgelösten Zustand anzeigt.</td></tr>
<tr><td>Alarm bei Auslösung eines Inputs</td><td>Ist ein Cause mit mehreren Input-TAGs projektiert, so kann der Benutzer wählen, ob ein Alarm angezeigt wird, sobald einer der Eingänge die Auslösekriterien erfüllt. Standardmäßig ist dies für diskrete und analoge Input-Typen folgendermaßen eingerichtet:<br>• Diskret: standardmäßig eingeschaltet<br>• Analog: standardmäßig eingeschaltet</td></tr>
<tr><td>Gegenseitig verriegelte TAG-Simulation</td><td>Wenn Sie diese Option aktivieren, ist die TAG-Simulation des Cause gegenseitig verriegelt. Dies bedeutet, dass jeweils nur ein TAG eines Cause simuliert werden kann.</td></tr>
</table>

### Zeitablaufdiagramm für Cause-Zeitfunktionen




Beachten Sie hierzu auch Kapitel "Übersicht zum Projektieren der Causes (Seite 83) ".

Ausführliche Darstellungen der Parametrierung und des Verhaltens der Causes siehe Kapitel "Beispielparametrierungen für Causes (Seite 163) ".

### 4.3.7 Dialog "Cause-Details" - Register "Alarme"

#### Voraussetzung

Voraussetzung für die Anzeige dieses Registers "Alarme" ist die Aktivierung des Kontrollkästchens "Platzieren für Cause und Effect" im Dialog "Eigenschaften" der Safety Matrix, Register "Alarme" (Menübefehl **Bearbeiten > Eigenschaften**).
Siehe Kapitel "Der Dialog "Eigenschaften" der Safety Matrix (Seite 75)".

#### Register "Alarme"

| Feld | Beschreibung |
|---|---|
| Alarm-Baustein platzieren | Mit diesem Kontrollkästchen wird der Meldebaustein F_SC_AL für diesen Cause platziert. |
| • Planzuordnung | Ordnen Sie ggf. in diesem Feld den Meldebaustein einer Technologischen Hierarchie zu. Mit Klick auf die zugehörige Schaltfläche "..." öffnet sich dafür ein Browser. |
| • Meldungen freigeben | Aktivieren Sie das Kontrollkästchen "Meldungen freigeben".<br>Mit Klick auf die zugehörige Schaltfläche "..." öffnet sich der Dialog für die Projektierung desjenigen vordefinierten Alarm-Profils für Causes und Effects, das im Register "Konfigurieren" ausgewählt ist. Dort können Sie<br>• einzelne Meldungen freigeben<br>• Meldeklassen ändern<br>• Prioritäten der Meldeklassen ändern<br>• die Quittieranforderung festlegen. |

Für die Zuordnung von Alarm-Profil zu Farbe für die Statusanzeige siehe Kapitel "Die Dialoge "Anpassen" (Seite 80)".

## 4.4 Projektieren der Effects

### 4.4.1 Übersicht zum Projektieren der Effects

#### Übersicht

Die Werte von mindestens einem und maximal vier diskreten Output-TAGs bilden die Wirkung auf den Prozess. Die Aktivierung eines Effect hängt von verschiedenen Faktoren ab:

- Typ des Schnittpunkts
- eingestellte Optionen des Effect

### 4.4.2 Effect und Spalte für Effect anlegen/ändern

#### Vorgehensweise zum Anlegen/Ändern eines Effect

Doppelklicken Sie im Konfigurationsbereich Effects der Safety Matrix auf eine (leere oder befüllte) Spalte oder klicken Sie auf die Spalte und wählen Sie "Ändern" im Kontextmenü. Der Dialog "Effect-Details - Effect x" wird geöffnet und Sie können den Effect anlegen oder ändern.

#### Das Kontextmenü im Konfigurationsbereich Effects der Safety Matrix

Wenn Sie im Konfigurationsbereich Effects der Safety Matrix auf eine Spalte klicken, so stellt Ihnen das Kontextmenü, je nach leerer oder bereits befüllter Spalte, die folgenden Funktionen zur Verfügung:

**Bei leerer Spalte:**

- Ändern Effect (der Dialog "Effect-Details - Effect x" wird geöffnet)
- Einfügen Spalte
- Löschen Spalte

**Bei befüllter Spalte:**

- Kopieren Effect
- Ausschneiden Effect
- Ändern Effect (der Dialog "Effect-Details - Effect x" wird geöffnet)
- Löschen Effect (der Effect, d. h. der Inhalt der Spalte wird gelöscht, aber die Spalte bleibt als leere Spalte erhalten)
- Einfügen Spalte (eine leere Spalte wird eingefügt und alle nachfolgenden Effects werden um eine Spalte nach unten verschoben)
- Löschen Spalte (die aktuelle Spalte wird gelöscht, und alle nachfolgenden Effects werden um eine Spalte nach oben verschoben)

---

**Hinweis**

Bei "Einfügen Spalte " wird die letzte Spalte der Safety Matrix immer gelöscht. Stellen Sie deshalb sicher, dass die letzte Spalte leer ist. Gegebenenfalls müssen Sie die Größe der Safety Matrix anpassen.

---

**Hinweis**

Bei "Einfügen Spalte " bzw. "Löschen Spalte " aktiviert das *Safety Matrix Engineering Tool* beim Transfer der Safety Matrix automatisch die Transfer-Option "Plan + Parameter". Beachten Sie dazu Kapitel "Transferieren der Safety Matrix in das Projekt (Seite 111)".

---

**Hinweis**

"Einfügen Spalte " bzw. "Löschen Spalte " kann dazu führen, dass in einem anschließenden Matrix-Vergleich alle nachfolgenden Spalten als geändert gekennzeichnet werden und somit bei einer Abnahme geprüft werden müssen. Sie können dies umgehen, indem Sie

- zusätzliche Effects immer am Ende hinzufügen
- nicht ganze Spalten ausschneiden, einfügen, kopieren, löschen, sondern nur deren Inhalte
- die Änderung der Größe der Safety Matrix vermeiden.

---

### 4.4.3 Übersicht über den Dialog "Effect-Details - Effect x"

#### Vorgehensweise zum Projektieren eines Effect

Doppelklicken Sie im Effects-Konfigurationsbereich der Safety Matrix auf eine (leere oder befüllte) Spalte oder klicken Sie auf die Spalte und wählen Sie "Ändern" im Kontextmenü. Der Dialog "Effect-Details - Effect x" wird geöffnet.

**Effect "x"**

Jedem Effect ist eine eindeutige Nummer innerhalb der Safety Matrix zugeordnet. Die Zuordnung erfolgt automatisch auf Grund der ausgewählten Spalte. Die Effect -Nummer kann nicht geändert werden.

#### Dialog zum Projektieren eines Effect

Der Dialog zum Projektieren eines Effect besteht aus den Registern:

- "Konfigurieren"
- "Optionen"
- "Alarme"

### 4.4.4 Dialog "Effect-Details" - Register "Konfigurieren"

#### Register "Konfigurieren"

<table>
<tr><th>Feld</th><th>Beschreibung</th></tr>
<tr><td>Beschr.</td><td>Alphanumerische Beschreibung des Effect, die bis zu 32 Zeichen lang sein kann. Die Eingabe der Beschreibung ist obligatorisch.</td></tr>
<tr><td>SIL (= Safety Integrity Level)</td><td>Dieses Feld dient zu Dokumentationszwecken. Hier können Sie den SIL für diesen Effect eintragen, den Sie in der Risikoanalyse (z. B. nach IEC 61508) ermittelt haben.<br>Eine Eingabe in diesem Feld ist nicht erforderlich. In der Voreinstellung ist kein SIL-Wert eingegeben..</td></tr>
<tr><td>TAG x</td><td>Geben Sie für jeden Effect mindestens einen TAG an. Beachten Sie dazu das Kapitel "Syntaxregeln für TAG-Namen in der Safety Matrix (Seite 55) ".</td></tr>
<tr><td>• (Schaltfläche) I/O</td><td>Mit Klick auf Schaltfläche "I/O" wird der Dialog "Auswahl I/O-TAG" geöffnet. Siehe Kapitel "Die TAGs der Safety Matrix (Seite 53)".</td></tr>
<tr><td>• (Schaltfläche) ...</td><td>Die Schaltfläche "..." erscheint, falls im Dialog "Auswahl I/O-TAG" die Option "Kanaltreiber" ausgewählt wurde. Mit Klick auf Schaltfläche "..." wird der Dialog "Kanaltreiber" geöffnet.<br>• Im Register "Parameter" können Sie für F-Kanaltreiber, die über Symbol ausgewählt werden:<br>  – festlegen, ob die Simulation Vorrang vor Fehler hat (Parameter SIM_MOD am F-Kanaltreiber F_CH_DO)<br>• Im Register "Optionen" können Sie<br>  – auswählen, ob Sie einen Startwert für die Simulation vorgeben möchten<br>  – ggf. einen Startwert für die Simulation dieses Output-TAG vorgeben.<br>Diese Parameter können auch direkt an den F-Kanaltreibern in den CFC-Plänen bearbeitet werden (inkl. Verschalten). Wenn Sie diese Möglichkeit nutzen, müssen Sie beachten, dass es dadurch zu Überschneidungen kommen kann. Die Daten, die in CFC gespeichert sind, haben Vorrang.</td></tr>
<tr><td>Aktion</td><td>In dieses Feld geben Sie einen Text mit bis zu 8 Zeichen ein, der beschreibt, welche Aktion veranlasst wird, wenn der Effect aktiv ist (zum Beispiel ÖFFNEN). Dieser Wert dient lediglich zur Anzeige/Dokumentation.</td></tr>
<tr><td>Energize-to-trip</td><td>Diese Option für die Output-TAGs legt fest, wann der Output-TAG auf "0" oder "1" gesetzt wird. In Deenergize-to-trip-Anwendungen wird der Output-TAG auf "0" gesetzt, wenn der Effect aktiv ist. In Energize-to-trip-Anwendungen wird der Output-TAG auf "1" gesetzt, wenn der Effect aktiv ist. Standardmäßig ist dieses Kontrollkästchen nicht aktiviert, d. h. die Voreinstellung ist Deenergize-to-trip, da der Wert "0" bei digitaler F-Peripherie als sichere Ruhelage gilt. Siehe folgende Tabelle.<br>Output-TAGs, für die Energize-to-trip aktiviert ist, sind in der Safety Matrix mit einem Sternchen (*) am Ende des Output-TAGs gekennzeichnet.</td></tr>
</table>

| Feld | Beschreibung |
|---|---|
| Funktionstyp | Mit dem "Funktionstyp" bestimmen Sie, unter welchen Bedingungen ein Effect aktiv wird. Die Eingabe in diesem Feld ist obligatorisch. |
| • Normal | Standardmäßig werden alle Effects und bis zu vier Output-TAGs auf die jeweiligen Werte gesetzt, wenn der Effect aktiv wird.<br>Hinweis: Der Funktionstyp "Normal" führt zu einem Auslösebefehl. Der Auslösebefehl kann zeitverzögert sein, bevor der Effect aktiv wird, er kann gesperrt und/oder umgangen werden. Siehe dazu "Dialog "Effect-Details" - Register "Alarme" (Seite 101) ". |
| • Nur Kommentar | Der Effect wird nicht verarbeitet. Nur zu Dokumentationszwecken. |
| Alarm-Profil | Jedem Effect ist ein Alarm-Profil zugeordnet. Sie können die Alarm-Profile für die Causes und Effects projektieren (siehe Kapitel "Dialog "Effect-Details" - Register "Alarme" (Seite 98)").<br>Die Wahl des Alarm-Profils entscheidet über die Farbdarstellung im Online-Betrieb und ggf. über die abgesetzten Meldungen des Effect. |
| • Standard | Alarm-Profil "Standard" wird eingestellt (Voreinstellung). |
| • Sequential | Alarm-Profil "Sequential" wird eingestellt. |

| Effect | Projektierung | Output-TAG |
|---|---|---|
| aktiv | DTT | 0 |
| | ETT | 1 |
| inaktiv | DTT | 1 |
| | ETT | 0 |

Beachten Sie hierzu auch Kapitel "Übersicht zum Projektieren der Effects (Seite 93)".

Ausführliche Darstellungen der Parametrierung und des Verhaltens der Effects, insbesondere unter Berücksichtigung der projektierten Schnittpunkttypen, siehe Kapitel "Beispielparametrierungen für Effects (Seite 167)".

## 4.4.5 Dialog "Effect-Details" - Register "Optionen"

### Register "Optionen"

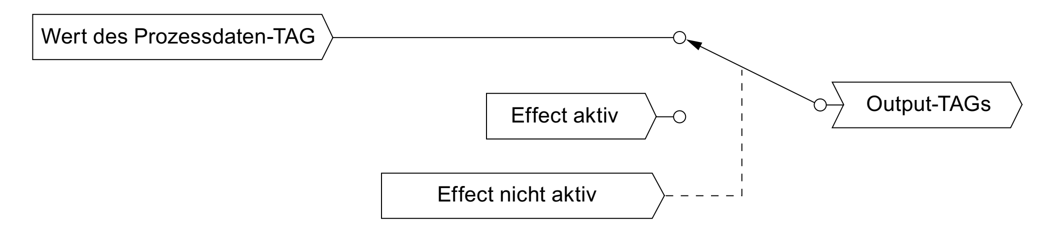
| Feld | Beschreibung |
|---|---|
| Ausgabeverzögerung | Ist das Kontrollkästchen "Freigeben" aktiviert, so werden die Ausgänge nach einer gewissen Zeitverzögerung ausgelöst. Die Dauer der Zeitverzögerung geben Sie im Eingabefeld "Dauer" an. Zum Löschen einer projektierten Ausgabeverzögerung müssen Sie die Freigabe zurücknehmen.<br>Hinweis: Die Ausgabeverzögerung wirkt nur auf die Output-TAGs des Effect, nicht auf die Aktivierung des Effect selbst. Bei der Visualisierung und bei internen Referenzen des Effect ist die Ausgabeverzögerung nicht maßgeblich. |
| Bypass | Die Effects können so konfiguriert werden, dass die folgenden Umgehungsfunktionen möglich sind: |
| • Soft-Bypass zulässig | Ist das Kontrollkästchen "Soft-Bypass zulässig" aktiviert, so kann der Bediener im Viewer oder im Online-Betrieb des Engineering Tools manuell einen Bypass für Wartungszwecke anlegen. In der Voreinstellung ist dieses Kontrollkästchen nicht aktiviert. |
| • Bypass-TAG | Mit Klick auf Schaltfläche "I/O" wird der Dialog "Auswahl I/O-TAG" geöffnet. Hier können Sie einen booleschen TAG als "Bypass-TAG" auswählen. Siehe Kapitel "Die TAGs der Safety Matrix (Seite 53)".<br>Für den Effect wird eine Umgehung aktiv, wenn der Wert des Bypass-TAG TRUE ist. Ein Bypass wird in der Regel für Wartungszwecke angelegt, z. B. bei Austausch eines Gebers. Im normalen Prozessbetrieb sollten Sie die Funktion "Übersteuern" verwenden.<br>Bei aktivem Bypass wird ein Effect deaktiviert, obwohl er aufgrund der anderen Bedingungen (Cause, Schnittpunkt) aktiv sein sollte. |
| Rücksetzen-/Übersteuern-TAG | Mit Klick auf Schaltfläche "I/O" wird der Dialog "Auswahl I/O-TAG" geöffnet. Hier können Sie einen booleschen TAG als "Rücksetzen-/Übersteuern-TAG" auswählen. Siehe Kapitel "Die TAGs der Safety Matrix (Seite 53)".<br>Der Effect kann übersteuert werden, wenn Schnittpunkttypen V oder R verwendet werden, oder er kann bei Verwendung der Schnittpunkttypen S oder R zurückgesetzt werden. Der Effect wird zurückgesetzt, wenn der Rücksetzen-/Übersteuern-TAG einen FALSE-TRUE-Übergang durchführt. Bei einem Übersteuern wird der Übersteuern-Status mit einem FALSE-TRUE-Übergang umgeschaltet. Siehe Kapitel "Dialog "Schnittpunktdetails" - Register "Konfigurieren" (Seite 103) " mit näheren Einzelheiten. |
| Maximale Zeit Übersteuern | In diesem Eingabefeld können Sie die maximale Zeit in Sekunden eingeben, für die der Effect im Übersteuern-Zustand bleiben kann. Sind die Bedingungen, die den Effect ausgelöst haben, nach Ablauf der maximalen Übersteuern-Zeit immer noch vorhanden, so wird der Effect wieder aktiv und ein Alarm "Fehler Überst.: Zeitüber." erscheint. Wird ein neuer Cause aktiv, der diesem Effect zugeordnet ist, so endet die Übersteuern-Funktion sofort, der Effect wird wieder aktiv und ein Alarm "Fehler Überst.: Cause" erscheint.<br>Die mit Maximale Zeit Übersteuern projektierte Zeit sollte nicht größer als die Dauer jeder beliebigen Bedingung sein, die der Prozess oder die Anlage toleriert. |

| Feld | Beschreibung |
|---|---|
| Zeit Vorwarnung Übersteuern | In diesem Eingabefeld können Sie die Zeit in Sekunden eingeben, nach der eine Vorwarnung für das Erreichen der **Maximalen Zeit Übersteuern** abgesetzt wird. Der betreffende Effect-TAG wird in der für "Vorwarnung" projektierten Farbe hinterlegt, wenn diese Zeit abgelaufen ist. |
| Maskierung oder Prozessdaten durchreichen | |
| • Aktiviert Prozesswert durchreichen | Wenn Sie dieses Kontrollkästchen aktivieren, wird der Effect für das Durchreichen des Prozesswertes projektiert. Dies setzt voraus, dass ein "Prozessdaten-TAG" angegeben ist. Siehe Beschreibung "Durchreichen des Prozesswerts" im Anschluss an diese Tabelle. |
| • Maskierungsfreigabe-TAG | Der Wert des Maskierungsfreigabe-TAG legt fest, ob die Effect-Logik oder eine extern gesteuerte Prozessvariable (siehe "Prozessdaten-TAG") mit den Output-TAGs des Effect verschaltet ist. Siehe Beschreibung "Maskierung" im Anschluss an diese Tabelle. |
| • Prozessdaten-TAG | Kennzeichnet eine externe Prozessvariable, die bei aktiviertem "Prozesswert durchreichen" an den Ausgang des Effect durchgereicht wird, wenn der Effect nicht aktiv ist. Dadurch kann ein Ausgang von einem Prozesswert gesteuert werden, bis eine Auslösebedingung den Effect aktiviert.<br>Ist ein Maskierungsfreigabe-TAG projektiert und dessen Wert TRUE, wird der Wert des Prozessdaten-TAG immer an die Output-TAGs durchgereicht.<br>Für Energize-to-trip (ETT)-Output-TAGs wird der Wert vom Prozessdaten-TAG invertiert, bevor er in die Output-TAGs geschrieben wird. |
| Kommentare | Es können zu jeder Safety Matrix 32 Anmerkungen eingegeben werden, die im Informationsbereich für Kommentare angezeigt werden. In den Feldern "Kommentare" können jedem Cause bis zu vier Anmerkungen zugeordnet werden. Die Zahl im Kästchen neben jedem Feld bezieht sich auf die zugehörige Anmerkung. |
| SIF-Gruppenzuordnung | Ein Effect kann bis zu vier SIF-Gruppen, das sind "Sicherheitstechnische Funktionsgruppen (**S**afety **I**nstrumented **F**unction groups)", zugeordnet werden. Eine SIF-Gruppe enthält zusammengehörige Causes und Effects, die typischerweise einer einzigen Sicherheitsschaltung aus Gebern, F-CPU und den Steuerungselementen, die eine bestimmte Sicherheitsfunktion ausführen, zugeordnet sind. Mit der Zuordnung zu einer SIF-Gruppe können Filterfunktionen für die Anzeige im Online-Betrieb für Causes und Effects realisiert werden.<br>Sie müssen die Sicherheitstechnischen Funktionsgruppen im Dialog "Eigenschaften" der Safety Matrix, Register "Allgemein" angelegt haben, bevor Sie sie hier zuordnen können. Bitte beachten Sie die Ausführungen dazu im Kapitel "Der Dialog "Eigenschaften" der Safety Matrix (Seite 75) ". |
| Gegenseitig verriegelte TAG-Simulation | Wenn Sie diese Option aktivieren, ist die TAG-Simulation des Effect gegenseitig verriegelt. Dies bedeutet, dass jeweils nur ein TAG eines Effect simuliert werden kann. |

## Durchreichen des Prozesswerts

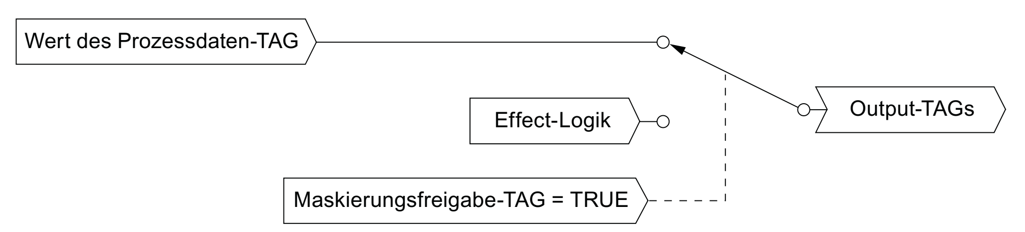
Dies ist ein Konzept, bei dem eine (von einem Steuerungssystem) extern gesteuerte Prozessvariable mit der Ausgangslogik des Effect verschaltet werden kann. Das Durchreichen des Prozesswerts wird von der Safety Matrix ignoriert, wenn der Effect aktiv wird. Durchreichen des Prozesswerts wird durch Aktivieren des Kontrollkästchens "Aktiviert Prozesswert durchreichen" und Eingabe eines Prozessdaten-TAG für die Prozessvariable projektiert.

Das Durchreichen wird durch den aktiven Zustand des Effect gesteuert, siehe nachfolgende Abbildung. Der Wert des Prozessdaten-TAG wird mit den Output-TAGs verschaltet, wenn die Effect-Logik nicht aktiv ist. Wird die Effect-Logik aktiv, so wird die Verschaltung des Prozessdaten-TAG-Wertes mit den Output-TAGs des Effect gelöst und der Ausgang wird von den fehlersicheren Werten angesteuert. Der fehlersichere Wert für einen Deenergize-to-trip (DTT)-Ausgang ist FALSE und für einen Energize-to-trip (ETT)-Ausgang ist er TRUE.




## Maskierung

Durch Maskierung des Effect können Sie die Effect-Logik mit dem Prozessdatenwert, wie im folgenden Bild gezeigt, übersteuern (Override). Die Übersteuern-Funktion wird durch den Wert des Maskierungsfreigabe-TAG gesteuert.




Die Projektierung eines Effect für die Maskierung setzt voraus, dass für "Maskierungsfreigabe-TAG" und "Prozessdaten-TAG" Werte eingegeben sind. Der Wert für den Maskierungsfreigabe-TAG legt fest, ob die Effect-Logik oder eine extern gesteuerte Prozessvariable (siehe "Prozessdaten-TAG") mit den Output-TAGs des Effect verschaltet wird.

Beachten Sie hierzu auch Kapitel "Übersicht zum Projektieren der Effects (Seite 93)".

Ausführliche Darstellungen der Parametrierung und des Verhaltens der Effects, insbesondere unter Berücksichtigung der projektierten Schnittpunkttypen, siehe Kapitel "Beispielparametrierungen für Effects (Seite 167)".

### 4.4.6 Dialog "Effect-Details" - Register "Alarme"

#### Voraussetzung

Voraussetzung für die Anzeige dieses Registers "Alarme" ist die Aktivierung des Kontrollkästchens "Platzieren für Cause und Effect" im Dialog "Eigenschaften" der Safety Matrix, Register "Alarme" (Menübefehl **Bearbeiten > Eigenschaften**).
Siehe Kapitel "Der Dialog "Eigenschaften" der Safety Matrix (Seite 75)".

#### Register "Alarme"

| Feld | Beschreibung |
|---|---|
| Alarm-Baustein platzieren | Mit diesem Kontrollkästchen wird der Meldebaustein F_SE_AL für diesen Effect platziert. |
| • Planzuordnung | Ordnen Sie ggf. in diesem Feld den Meldebaustein einer Technologischen Hierarchie zu. Mit Klick auf die zugehörige Schaltfläche "..." öffnet sich dafür ein Browser. |
| • Meldungen freigeben | Aktivieren Sie das Kontrollkästchen "Meldungen freigeben".<br>Mit Klick auf die zugehörige Schaltfläche "..." öffnet sich der Dialog für die Projektierung desjenigen vordefinierten Alarm-Profils für Causes und Effects, das im Register "Konfigurieren" ausgewählt ist. Dort können Sie<br>• einzelne Meldungen freigeben<br>• Meldeklassen ändern<br>• Prioritäten der Meldeklassen ändern<br>• die Quittieranforderung festlegen. |

Für die Zuordnung von Alarm-Profil zu Farbe für die Statusanzeige siehe Kapitel "Die Dialoge "Anpassen" (Seite 80)".

# 4.5 Projektieren der Schnittpunkte

## 4.5.1 Bearbeiten oder Ändern von Schnittpunkten

### Schnittpunkt bearbeiten oder ändern

Wählen Sie eine gültige Schnittpunkt-Zelle im Schnittpunkt eines projektierten Cause und eines projektierten Effect. Jede Safety Matrix unterstützt bis zu 1024 Schnittpunkte.

### Vorgehensweise zum Bearbeiten/Ändern eines Schnittpunkts

Doppelklicken Sie im Schnittpunkte-Konfigurationsbereich der SafetyMatrix auf einen (leeren oder befüllten) Schnittpunkt oder klicken Sie auf den Schnittpunkt und wählen Sie "Ändern Schnittpunkt" im Kontextmenü.
Der Dialog "Schnittpunktdetails - Cause x, Effect x" wird geöffnet und Sie können den Schnittpunkt anlegen oder ändern.

### Das Kontextmenü im Schnittpunkte-Konfigurationsbereich der Safety Matrix

Wenn Sie im Schnittpunkte-Konfigurationsbereich der Safety Matrix auf einen Schnittpunkt klicken, so stellt Ihnen das Kontextmenü, je nach leerem oder bereits befülltem Schnittpunkt, die folgenden Funktionen zur Verfügung:

**Bei leerem Schnittpunkt eines projektierten Cause und eines projektierten Effect:**

- Ändern Schnittpunkt
- Einfügen Schnittpunkt
- N - Nicht speichernd
- S - Speichernd
- V - Übersteuerbar
- R - Rücksetzbar und übersteuerbar
- X - Nicht spezifiziert
- * - Nur Kommentar
- XooN (X spezifizieren)

**Bei befülltem Schnittpunkt eines projektierten Cause und eines projektierten Effect:**

- Kopieren Schnittpunkt
- Ausschneiden Schnittpunkt
- Ändern Schnittpunkt
- Löschen Schnittpunkt
- N - Nicht speichernd
- S - Speichernd
- V - Übersteuerbar
- R - Rücksetzbar und übersteuerbar
- X - Nicht spezifiziert
- * - Nur Kommentar
- Keine
- XooN (X spezifizieren)

### 4.5.2 Dialog "Schnittpunktdetails" - Register "Konfigurieren"

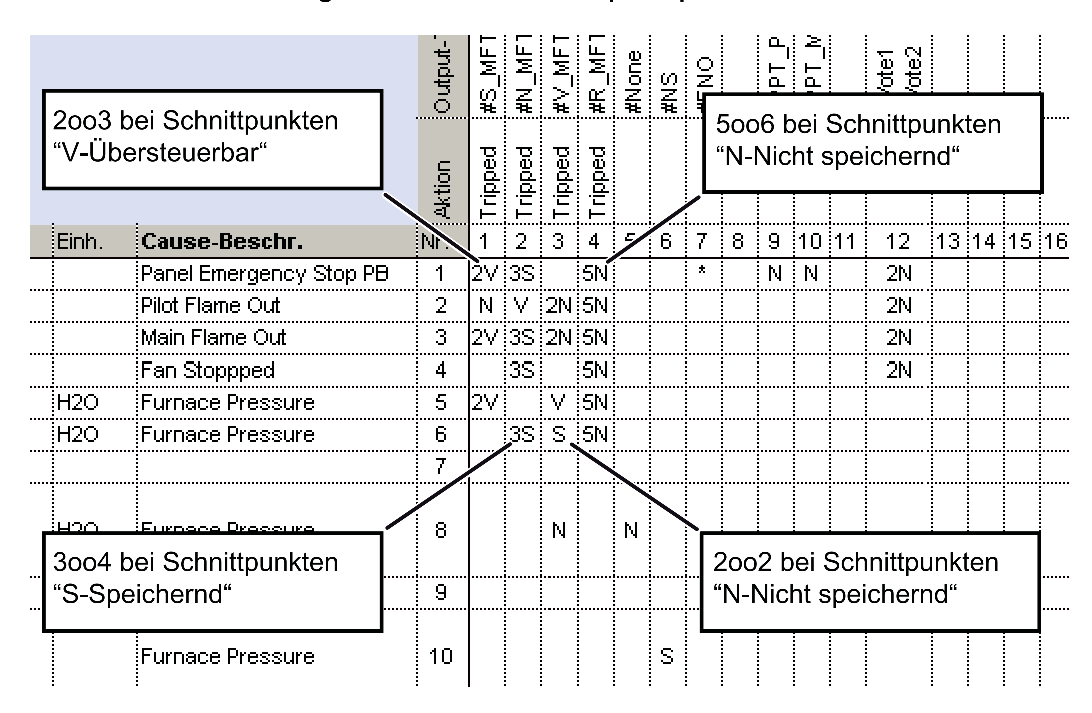
#### Vorgehensweise zum Bearbeiten/Ändern eines Schnittpunkts

Doppelklicken Sie im Schnittpunkte-Konfigurationsbereich der Safety Matrix auf einen (leeren oder befüllten) Schnittpunkt oder klicken Sie auf den Schnittpunkt und wählen Sie "Ändern Schnittpunkt" im Kontextmenü.
Der Dialog "Schnittpunktdetails - Cause x, Effect x" wird geöffnet und Sie können den Schnittpunkt anlegen oder ändern.

#### Register "Konfigurieren"

| Feld | Beschreibung |
|---|---|
| N - Nicht speichernd | Einfache Durchgangsfunktion. Ist der Cause aktiv, wird der Effect ausgelöst. |
| S - Speichernd | Ist der Cause aktiv, wird der Effect ausgelöst und gespeichert. Wird der Effect nicht mehr ausgelöst, so muss er vom Bediener im Viewer oder im Online-Betrieb des Engineering Tools manuell, oder durch Setzen des projektierten Rücksetzen/Übersteuern-TAG auf TRUE gelöscht werden. |
| V - Übersteuerbar | Ist der Cause aktiv, wird der Effect ausgelöst. Sie können die Auslösung des Effect übergehen durch<br>• manuellen Eingriff oder<br>• durch Setzen des projektierten Rücksetzen/Übersteuern-TAG auf TRUE, solange der Effect noch ausgelöst wird. |
| R - Rücksetzbar und übersteuerbar | Dieser Schnittpunkttyp ist eine Verbindung der oben beschriebenen Typen S und V. Die mit diesem Schnittpunkttyp verschalteten Effects bleiben aktiv, wenn der zugehörige Cause inaktiv wird, können jedoch<br>• solange der Cause aktiv ist, mit der Übersteuern-Funktion übergangen bzw.<br>• wenn der Cause nicht mehr aktiv ist, quittiert werden. |
| X - Nicht spezifiziert | Es ist eine Verbindung zwischen dem Cause und dem Effect erforderlich, aber der gewünschte Schnittpunkttyp ist noch nicht festgelegt. Es wird keine Verbindung verarbeitet, bis der Schnittpunkttyp eingegeben ist. Eine Safety Matrix mit Schnittpunkttyp X kann nicht an die CPU übertragen werden. |
| * - Nur Kommentar | Es wird keine Verbindung zwischen diesem Cause und diesem Effect verarbeitet. Nur zu Dokumentationszwecken. |
| Keine | Es besteht keine Verbindung zwischen diesem Cause und diesem Effect (kein Eintrag im Schnittpunkt). Dies ist der voreingestellte Schnittpunkttyp. |
| XooN Wert (2-15) | Damit können Causes nach dem Mehrheitsverfahren zugeordnet werden. X wird vom Benutzer eingegeben, N wird bestimmt anhand der Anzahl der Schnittpunkte mit X als Koeffizienten.<br>Zu jedem Effect ist nur eine XooN-Zuordnung zulässig. Es können für die Zuordnung nach dem Mehrheitsprinzip nur Schnittpunkte gleichen Typs (zum Beispiel alle S oder alle N) berücksichtigt werden. Beispiele für diese Art der Schnittpunktzuordnung zeigt die folgende Abbildung. |

## Beispiele für die Schnittstellenzuordnung nach dem Mehrheitsprinzip




### Hinweis

Die Safety Matrix bietet ein bequemes Verfahren für die Sammelverarbeitung der Sicherheitslogik. Bei Bedarf können alle Effects gleichzeitig aktiviert werden. Dies ist möglich, indem Sie einen einzigen Cause projektieren und durch einen Schnittpunkt mit allen Effects verschalten. Wird dieser Cause aktiv, so löst er jede Effect-Logik aus (einschließlich projektierter Zeitverzögerungen).

Ausführliche Darstellungen der Parametrierung und des Verhaltens der Effects, insbesondere unter Berücksichtigung der projektierten Schnittpunkttypen, siehe Kapitel "Beispielparametrierungen für Effects (Seite 167)".

## 4.6 Importieren/Exportieren einer Cause/Effect-Matrixdatei

### Importieren

Beim Anlegen und Überarbeiten von Safety Matrizen kann es erforderlich sein, die außerhalb eines SIMATIC-Projekts entwickelte Matrixlogik in das S7-Programm einzufügen. Dies wird als das "Importieren einer Safety Matrix" bezeichnet.

Ein Beispiel ist etwa eine generische Cause/Effect-Matrix für eine Notabschaltung, die in einer unternehmensinternen Forschungs- und Entwicklungsabteilung entwickelt wurde und in einer Reihe verschiedener Standorte zur Einbindung in ein lokales Projekt installiert werden soll.

### Exportieren

Eine erstellte Safety Matrix kann auf einem PC außerhalb von *PCS 7* bzw. *STEP 7* überprüft und weiterbearbeitet werden. Dazu müssen Sie Ihre Safety Matrix in eine Cause/Effect-Matrixdatei (.cem) exportieren.

Beispielsweise kann an einer Workstation mit dem *Safety Matrix Engineering Tool* die Anfangsversion einer Safety Matrix erstellt werden. Die Logik der Safety Matrix kann gespeichert und für die lokale Überarbeitung als Email an entfernte Kollegen verschickt werden.

### 4.6.1 Importieren einer Cause/Effect-Matrixdatei (.cem) in ein PCS 7-Projekt

### Einleitung

Alle Matrizen, die mit dem Safety Matrix Editor erstellt und bearbeitet wurden, müssen auf diesem Weg in ein SIMATIC-Projekt importiert werden.

Für den Transport benötigen Sie die Matrix im Format einer Cause/Effect-Matrixdatei (.cem). Die .cem-Datei enthält die gesamten Konfigurationsdaten für jeweils eine Safety Matrix.

---

**Hinweis**

Der (Re-)Import einer Matrixdatei ist nicht möglich, falls bereits ein gleichnamiger *CFC*-Plan besteht. In diesem Fall müssen Sie **vor** dem (Re-)Import der Matrixdatei den *CFC*-Plan umbenennen (im S7-Programm, Ordner **Pläne**) und danach wieder zurück benennen.

---

| ACHTUNG |
| --- |
| Wenn Sie den vorhandenen *CFC*-Plan löschen, gehen damit auch etwaige vorgenommene Verschaltungen zum *CFC*-Plan der Safety Matrix verloren. |

### Vorgehensweise

Zum Importieren der .cem-Matrixdatei in ein SIMATIC-Projekt gehen Sie folgendermaßen vor:

1. Starten Sie den *SIMATIC Manager*.
2. Öffnen Sie das Projekt, in das die Safety Matrix importiert werden soll.
3. Markieren Sie im S7-Programm den Ordner **Matrizen**und öffnen Sie die Objekteigenschaften.
4. Öffnen Sie das Register "Matrix".
5. Klicken Sie auf die Schaltfläche "Import CEM".
6. Wählen Sie im folgenden Auswahlfenster die gewünschte zu importierende .cem-Datei aus.

#### Ergebnis

Die importierte Safety Matrix-Datei erscheint im Ordner **Matrizen**und lässt sich wie andere Safety Matrizen bearbeiten, transferieren, übersetzen und laden.

### Siehe auch

Safety Matrix Editor (Seite 107)

## 4.6.2 Exportieren einer Cause/Effect-Matrixdatei (.cem)

### Vorgehensweise

Zum Exportieren der Safety Matrix in eine .cem-Matrixdatei gehen Sie folgendermaßen vor:

- Wählen Sie im *Safety Matrix Engineering-Tool* den Menübefehl **Datei > Speichern als** und geben Sie den gewünschten Namen und Speicherplatz der .cem-Datei ein.

Oder:

1. Starten Sie den *SIMATIC Manager*.
2. Öffnen Sie das Projekt, in das die Safety Matrix importiert werden soll.
3. Markieren Sie im S7-Programm im Ordner **Matrizen** die zu exportierende Matrix und betätigen Sie die rechte Maustaste.
4. Wählen Sie den Eintrag **Quelle exportieren**.
5. Wählen Sie im folgenden Auswahlfenster den gewünschten Namen und Speicherplatz für die zu exportierende Safety Matrix.

# 4.7 Safety Matrix Editor

## Funktionalität

Der *Safety Matrix Editor* ist eine Untermenge des *Safety Matrix Engineering Tools*. Seine Funktionalität ist auf das Projektieren einer Safety Matrix außerhalb der SIMATIC-Umgebung beschränkt. Der Safety Matrix Editor unterstützt die Überprüfung der Cause- und Effect-Logik.

## Beispiel

Beispielsweise kann an einer Workstation mit dem *Safety Matrix Engineering Tool* die Anfangsversion einer Safety Matrix erstellt werden. Die Logik der Matrix kann gespeichert und für die lokale Überarbeitung über das Netzwerk gemeinsam genutzt oder als Email an entfernte Kollegen verschickt werden. Mit dem *Safety Matrix Editor* kann der Bearbeiter die Safety Matrix öffnen und im gleichen Format wie der Ersteller betrachten. Der Bearbeiter kann die Safety Matrix-Konfiguration ändern (z. B. Funktionstypen ändern, Parameter verändern, Kommentare einfügen) und speichern. Eine Safety Matrix kann auch aus dem *Safety Matrix Editor* hervorgehen.

Schließlich kann die Safety Matrix in ein SIMATIC-Projekt eingebunden werden, siehe Kapitel "Importieren/Exportieren einer Cause/Effect-Matrixdatei (Seite 105) ".

## Einschränkungen im Funktionsumfang

Die folgenden Funktionen des *Safety Matrix Engineering Tools* sind im *Safety Matrix Editor* **nicht** vorhanden:

- Transferieren in das Projekt
- Übersetzen
- Laden
- Safety Matrix vergleichen mit
  - SIMATIC Projekt
  - CPU
- Vergleich zweier Safety Matrizen auf der Basis der erzeugten Pläne
- Beobachten

## Den Safety Matrix Editor öffnen

Wählen Sie den Windows-Befehl **Start > Programme > Siemens > SafetyMatrix**.

## Anlegen einer neuen Safety Matrix

Wählen Sie den Menübefehl **Datei > Neu**.

Es wird ein Dialog geöffnet, in dem Sie aufgefordert werden, einen Namen für die neue Safety Matrix einzugeben.

Standardmäßig wird die neue Safety Matrix im Verzeichnis C:\Siemens\SafetyMatrix abgelegt. Sie können aber auch einen anderen Speicherplatz wählen.

## Eine vorhandene Safety Matrix-Datei öffnen

1. Wählen Sie **Datei > Öffnen**.
2. Gehen Sie zu der gewünschten Safety Matrix-Datei.
3. Markieren Sie die Datei und öffnen Sie sie.

## Eine Safety Matrix bearbeiten

Nach dem Öffnen einer Safety Matrix zur Bearbeitung funktioniert das Projektieren im *Safety Matrix Editor* auf die gleiche Weise wie im *Safety Matrix Engineering Tool*.

## Eine Safety Matrix-Datei gemeinsam nutzen

Die Safety Matrix ist vollständig in der Cause/Effect-Matrixdatei (.cem) enthalten. Sie kann wie jede beliebige Datei mit den bekannten Systemfunktionen verschoben, kopiert usw. werden. Die .cem-Datei kann an einem gemeinsam genutzten Ablageort zugänglich gemacht oder an andere Benutzer per Email verschickt werden.

Sie können eine Safety Matrix-Datei nicht gleichzeitig von zwei *Safety Matrix-Editoren* bearbeiten.

## Siehe auch

Importieren einer Cause/Effect-Matrixdatei (.cem) in ein PCS 7-Projekt (Seite 105)

# 5 Zugriffschutz

## Zweck und Funktionsweise

Der Zugriffschutz schützt S7 F/FH Systems vor unbefugtem Zugriff, z. B. gegen unerwünschtes Herunterladen in die F-CPU (Downloads) vom Engineering System (ES). Zusätzlich zum Passwort für die F-CPU benötigen Sie für S7 F/FH Systems ein weiteres Passwort für das Sicherheitsprogramm.

Die folgenden Tabellen beschreiben das Passwort für die F-CPU und das Passwort für das Sicherheitsprogramm.

| Passwort für F-CPU | |
|---|---|
| Vergabe des Passworts | In *HW Konfig*, bei der Projektierung der F-CPU im Register "Schutz" des Dialogs "Eigenschaften" |
| Abfrage des Passworts beim | • Laden des gesamten S7-Programms aus dem *Safety Matrix Engineering Tool*<br>• Laden von Änderungen des Sicherheitsprogramms aus dem *Safety Matrix Engineering Tool* |
| Gültigkeit des Passworts | Die Zugangsberechtigung ist so lange gültig, bis sie ausdrücklich über die entsprechende Funktion des *SIMATIC Managers* (Menübefehl **Zielsystem > Zugangsberechtigung > Aufheben**) zurückgenommen wird oder Sie die letzte *STEP 7*-Anwendung beenden.<br>Die Zugangsberechtigung kann ungültig werden, wenn die Hardware-Konfiguration der F-CPU geändert und geladen wird. |

| Passwort für Sicherheitsprogramm | |
|---|---|
| Vergabe des Passworts | Im *SIMATIC Manager*, Menü **Extras > Sicherheitsprogramm bearbeiten** |
| Abfrage des Passworts beim | • Speichern von kritischen Änderungen einer Safety Matrix<br>• Transferieren einer Safety Matrix in das Sicherheitsprogramm<br>• Übersetzen von Änderungen am Sicherheitsprogramm<br>• Laden von Änderungen am Sicherheitsprogramm<br>• Starten der ersten Bedienung über Secure Write im Online-Betrieb des *Safety Matrix Engineering Tools*<br>• Deaktivieren und Aktivieren des Sicherheitsbetriebs |
| Gültigkeit des Passworts | Die Zugangsberechtigung besteht nach korrekter Eingabe des Passworts eine Stunde lang, verlängert sich nach jeder passwortpflichtigen Aktion auf eine Stunde oder bis zur ausdrücklichen Aufhebung der Zugangsberechtigung im *SIMATIC Manager* (Menübefehl **Extras > Sicherheitsprogramm bearbeiten**, dann Schaltfläche **Passwort**, dann Schaltfläche **Zugangsberechtigung aufheben**). |

Eine ausführliche Darstellung dieses Zugriffschutzes finden Sie im Programmier- und Bedienhandbuch "S7 F/FH Systems, Projektieren und Programmieren (http://support.automation.siemens.com/WW/view/de/2201072)".

# 6 Safety Matrix transferieren

### Einleitung

Der Transfer einer Safety Matrix in das Projekt beinhaltet

- das Speichern der Safety Matrix mit Prüfung der Projektierung auf Plausibilität
- das Erzeugen einer F-Systems-Programmlogik auf *CFC*-Basis mit Bausteinen aus der Safety Matrix-Bausteinbibliothek.

### Hierarchischer Plan

Nach dem Transfer existiert für jede Safety Matrix ein *CFC*-Basisplan mit zwei hierarchischen Plänen:

- hierarchischer Plan der Kanaltreiber ("MatrixName")
- hierarchischer Plan der Matrixlogik ("@MatrixName"). Dieser Plan ist geschützt, d. h. er kann nicht im *CFC* geöffnet werden.

## 6.1 Transferieren der Safety Matrix in das Projekt

Nach der vollständigen Projektierung einer Safety Matrix muss die Safety Matrix gespeichert und in das Projekt transferiert werden, bevor sie übersetzt und zur Ausführung in die F-CPU geladen wird.

### Transferieren der Safety Matrix in ein Projekt

1. Wählen Sie den Menübefehl **Datei > Transferieren**.
2. Optional: Wählen Sie im folgenden Dialog die Transfer-Optionen "Plan + Parameter" und/oder "Importierte Kanaltreiber verwenden (IEA Unterstützung)" und/oder "Hierarchische Plan-Anschlüsse bereinigen".
3. Starten Sie den Transfer-Vorgang, indem Sie die Schaltfläche **OK** betätigen.
4. Ordnen Sie den erzeugten Safety Matrix-Basisplan einem Hierarchieordner in der Technologischen Hierarchie zu, indem Sie ihn von der Komponentensicht in die Technologische Sicht verschieben. (Siehe Projektierungshandbuch "Prozessleitsystem PCS7 Engineering System (http://support.automation.siemens.com/WW/view/de/24450116)", Kap. 7.5.10.)

Führen Sie die Schritte 1 bis 3 für jede zu transferierende Safety Matrix durch.

## Transfer-Optionen

Die Option "Plan + Parameter" löscht den gesamten hierarchischen Plan der Matrixlogik ("@MatrixName") und legt einen neuen an. Diese Option wird vom *Safety Matrix Engineering Tool* vorgegeben und kann nicht mehr abgewählt werden, wenn:

- die Größe der Safety Matrix geändert wurde
- eine Cause-Zeile oder eine Effect-Spalte eingefügt oder gelöscht wurde

Die Option "Plan + Parameter" können Sie beim Transfer auch optional wählen (siehe unten).

---

**Hinweis**

Im Log-Fenster zum Transfer erkennen Sie am Eintrag "Erstellen des Matrix-Plans im Projekt", dass der Transfer mit der Transfer-Option "Plan + Parameter" durchgeführt wurde. Überprüfen Sie diesen Eintrag anhand der Parametrierung.

---

## Option "Parameter"

Änderungsladen an einer laufenden Safety Matrix können Sie durchführen, wenn Sie mit der Option "Parameter" transferiert haben. Die Bearbeitung der nicht geänderten Causes, Effects und Schnittpunkte bleibt hiervon unbeeinflusst.

Bei den geänderten Causes und Effects müssen Sie Folgendes beachten:

- Beim Änderungsladen in die F-CPU bleiben gespeicherte Informationen (z. B. aktive Zeiten, Meldungen) erhalten. Dies kann zu Kollisionen zwischen alter und neuer Projektierung führen!
  Beispiel: Wenn der alte Effect speichernd aktiv war und neu als nicht speichernd projektiert wurde, kann dieser Effect wegen des fehlenden Rücksetzen-TAGs nicht mehr zurückgesetzt werden.
- Ist dieses Verhalten nicht gewünscht, müssen Sie das Änderungsladen in zwei Schritten durchführen:
  - zuerst die Projektierungen der betroffenen Causes/Effects löschen und laden
  - danach die neue Konfiguration projektieren und laden




**Auswirkung auf Änderungsladen**

Wenn Sie die Transfer-Option "Parameter" aktiviert haben, müssen Sie sicher sein, dass keine oben erwähnten Kollisionen bei den geänderten Causes/Effects auftreten. Im Zweifelsfall aktivieren Sie die Transfer-Option "Plan + Parameter".

Die Transfer-Option "Parameter" dürfen Sie nur aktivieren, wenn die von Ihnen getätigten Änderungen nachvollziehbar sind.

### Option "Plan + Parameter"

Wenn Sie mit der Option "Plan + Parameter" transferieren, müssen Sie Folgendes beachten:

- Wenn Sie diese Safety Matrix anschließend per Änderungsladen in die F-CPU laden, läuft die Safety Matrix komplett mit Initialdaten neu an:
  - sämtliche gespeicherten Informationen (z. B. aktive Zeiten, Meldungen) gehen verloren
  - die Output-TAGs der neu geladenen Safety Matrix F-Bausteine geben nach dem Erstlauf den aus der Safety Matrix-Logik errechneten Wert aus
  - bei Rückkopplungen von Causes/Effects haben die entsprechenden TAGs im Erstlauf den Wert FALSE, wenn Sie:

    - in einem Cause einen Effect referenzieren

    - in einem Cause einen anderen Cause mit größerer Nummer referenzieren
  - Output-TAGs der Safety Matrix haben vor dem Erstlauf den Wert FALSE. Dies ist nur wichtig, falls diese TAGs in der Ablaufreihenfolge **vor** der Safety Matrix ausgewertet werden.
- Die Bearbeitung der Safety Matrix wird während des Änderungsladens in die F-CPU unterbrochen, planen Sie daher in dieser Zeit keine aktive Prozessführung durch die Safety Matrix (alle Effects im nicht aktivierten Zustand).
- Ein Änderungsladen in die OS ist danach zwingend erforderlich. An dieser OS ist während dieser Zeit ebenfalls keine aktive Prozessführung durch die Safety Matrix möglich.




**Transfer mit Option "Plan + Parameter"**

Ein Transfer mit der Option "Plan + Parameter" resultiert immer in einer geänderten F-Systems-Gesamtsignatur, auch dann, wenn die Projektierung der Safety Matrix nicht geändert wurde!

### Option "Importierte Kanaltreiber verwenden (IEA Unterstützung)"

Externe F-Kanaltreiber sind F-Kanaltreiber, die nicht durch die Safety Matrix platziert wurden. Damit die Safety Matrix auch externe F-Kanaltreiber als 'eigene Kanaltreiber' verschaltet, müssen Sie beim Transfer der Safety Matrix in das Projekt die Option "Importierte Kanaltreiber verwenden (IEA Unterstützung)" aktivieren. Erst dadurch wirkt sich die Funktion "TAG simulieren" auch auf diese externen F-Kanaltreiber aus, und die Reintegration der Module nach quittierpflichtigen Fehlern vom *Safety Matrix Viewer* oder im Online-Betrieb des *Safety Matrix Engineering Tools* über die Schaltfläche **Treiber quitt.** bezieht auch diese externen F-Kanaltreiber mit ein.

### Option "Hierarchische Plan-Anschlüsse bereinigen"

Beim Transfer mit der aktivierten Option "Hierarchische Plan-Anschlüsse bereinigen" werden Anschlüsse am hierarchischen Plan der Safety Matrix gelöscht, die intern nicht mehr verwendet werden. Beachten Sie, dass dabei die von Ihnen erstellten Verbindungen zu diesen Anschlüssen des hierarchischen Plans der Safety Matrix verloren gehen.

## Option "Alarm-Bausteine platzieren"

Beim Transfer mit der aktivierten Option "Alarm-Bausteine platzieren" werden die projektierten Meldebausteine im *CFC*-Plan platziert.

---

**Hinweis**

Ist das Kontrollkästchen "Platzieren" der Alarm-Bausteine **nicht** aktiviert, werden beim Transfer die vorhandenen Meldebausteine gelöscht und keine neuen Meldebausteine platziert. Es erfolgen keine Meldungen und es werden keine Bausteinsymbole für die OS angelegt. Dies gilt auch, wenn innerhalb der Safety Matrix die Meldebausteine F_MA_AL (Safety Matrix, 1-mal), F_SC_AL (Causes, x-mal) und F_SE_AL (Effects, x-mal) korrekt projektiert wurden.

---

### Voraussetzung für das Erzeugen von Bausteinsymbolen

Voraussetzung für das Erzeugen der Bausteinsymbole für die Safety Matrix ist die entsprechende Projektierung der Meldebausteine (siehe Kapitel "Meldungsprojektierung (Seite 61)") und der Transfer der Safety Matrix mit aktivierter Option "Alarm-Bausteine platzieren".

### Zusatzoptionen

Zusätzlich können Sie eine von drei Optionen auswählen:

- **Alle aktualisieren (Empfehlung)**:
  Die aktuelle Projektierung der Meldebausteine in der Safety Matrix wird in das *CFC*-Programm transferiert. Meldebausteine werden (neu) platziert, nicht mehr verwendete gelöscht.
- **Neue aktualisieren**:
  Es werden nur die neu erstellten Meldebausteine in das *CFC*-Programm transferiert. Nicht mehr verwendete Meldebausteine werden gelöscht.
- **Unverändert lassen**:
  Die aktuelle Projektierung der Meldebausteine in der Safety Matrix wird ignoriert. Es werden keine Meldebausteine neu platziert oder gelöscht.

## Transfer der Safety Matrix

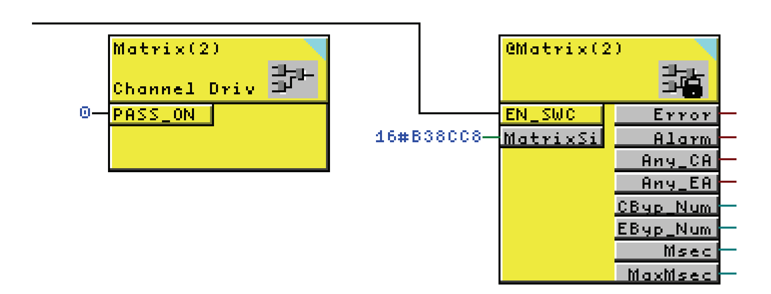
Beim Transfer wird die Safety Matrix auf Projektierungsfehler überprüft, wie etwa Causes ohne Schnittpunkte. Die Ergebnisse der Überprüfung werden im Log-Fenster angezeigt. Das Log-Fenster des Transfer-Vorgangs öffnen Sie mit der Schaltfläche **Zeige Details**.

Ist die Überprüfung in Ordnung, so führt das *Safety Matrix Engineering Tool* einen Vergleich zwischen der aktuellen Safety Matrix und der im Projekt gespeicherten Safety Matrix durch. Die Unterschiede werden im Log-Fenster angezeigt. Sie werden aufgefordert, die Änderungen zu überprüfen, bevor der Transfer fortgesetzt wird.

### Ergebnis

Beim Transfer wird im SIMATIC-Projekt ein *CFC*-Basisplan mit dem Namen der Safety Matrix angelegt. Der Plan enthält einen geschützten hierarchischen Plan ("@MatrixName") mit der vollständigen Konfiguration der Safety Matrix. Ein zweiter hierarchischer Plan ("MatrixName") enthält die automatisch angelegten F-Kanaltreiber. Die F-Kanaltreiber, die mittels IEA-Support verschaltet wurden, werden nicht hierher verschoben.

Die folgende Abbildung zeigt den beim Transfer einer Safety Matrix mit dem Namen "Matrix(2)" erzeugten Plan.



## Hierarchischer Plan der Kanaltreiber ("MatrixName")

Das *Safety Matrix Engineering Tool* platziert während des Transfers in einen *CFC*-Plan automatisch die folgenden F-Kanaltreiber aus *S7 F Systems*:

- F_CH_DI für diskrete Cause-TAGs: F-Kanaltreiber für digitale Eingänge von F-Peripherien (ausgenommen fehlersichere DP-Normslaves und PA-Feldgeräte*)
- F_CH_AI für analoge Cause-TAGs: F-Kanaltreiber für analoge Eingänge von F-Peripherien (ausgenommen fehlersichere DP-Normslaves und PA-Feldgeräte*)
- F_CH_DO für Effect-TAGs: F-Kanaltreiber für digitale Ausgänge von F-Peripherien (ausgenommen fehlersichere DP-Normslaves und PA-Feldgeräte*)

  * Falls Sie fehlersichere DP-Normslaves oder fehlersichere PA-Feldgeräte in einer Safety Matrix verwenden, platzieren Sie die F-Kanaltreiber dafür manuell und verschalten Sie sie über Plananschlüsse am hierarchischen Plan der Matrixlogik mit der Safety Matrix.

Der hierarchische Plan der Kanaltreiber hat einen sichtbaren Eingang:

- Eingang PASS_ON ist mit allen internen F-Kanaltreibereingängen PASS_ON verschaltet. Über eine Verschaltung dieses Eingangs können Sie alle F-Kanaltreiber der Safety Matrix passivieren, z. B. wenn Sie eine Passivierung abhängig von bestimmten Zuständen in Ihrem Sicherheitsprogramm aktivieren möchten.

Die unsichtbaren Plananschlüsse (Eingänge und Ausgänge) dürfen nicht verändert werden.




**Hierarchischer Plan der Kanaltreiber**

Sie dürfen den hierarchischen Plan der Kanaltreiber ("MatrixName") nicht umbenennen, kopieren oder verschieben.
Außerdem dürfen Sie darin keine Verschaltungen löschen.

---

Hinweis

**Neue Verschaltungen im hierarchischen Plan der Kanaltreiber ("MatrixName") dürfen nicht hinzugefügt werden**

Sie dürfen an den F-Kanaltreibern keine internen Verschaltungen hinzufügen, da diese bei einem nachfolgenden Transfer mit gesetzter Option "Plan + Parameter" wieder gelöscht werden.
Verschaltungen an F-Kanaltreibern außerhalb des hierarchischen Plans der Kanaltreiber bleiben erhalten.

---

Hinweis

**Bausteine im hierarchischen Plan der Kanaltreiber ("MatrixName") dürfen nicht geändert, umbenannt, hinzugefügt oder gelöscht werden**

Sie dürfen im hierarchischen Plan der Kanaltreiber keine Bausteine ändern, umbenennen, hinzufügen oder löschen.

---

### Hierarchischer Plan der Matrixlogik ("@MatrixName")

Der hierarchische Plan der Matrixlogik hat immer mindestens **zwei Eingänge**:

- MatrixSig: Enthält die Safety Matrix-Signatur
- EN_SWC: Über diesen Eingang (F_BOOL) kann die Funktion Secure Write für das Bedienen im Online-Betrieb des Engineering Tools und von der PCS 7 OS mittels eines vor dem Übersetzen im *CFC* verdrahteten Signals freigegeben (= TRUE) und ggf. auch abgebrochen werden. Siehe Kapitel " Secure Write (Seite 136) ".

Der hierarchische Plan der Matrixlogik hat immer mindestens **acht Ausgänge**:

- Error – Boolescher Merker, der anzeigt, dass ein Fehler im Sicherheitsdatenformat erkannt wurde
- Alarm – Boolescher Merker, der anzeigt, dass eine Alarmbedingung erkannt wurde
- Any_CA – Zeigt an, dass mindestens einer der Causes in der Safety Matrix aktiv ist
- Any_EA – Zeigt an, dass mindestens einer der Effects in der Safety Matrix aktiv ist
- CByp_Num – Ganzzahliger Wert, der anzeigt, wie viele Causes aktuell mit Bypass geschaltet sind
- EByp_Num – Ganzzahliger Wert, der anzeigt, wie viele Effects aktuell mit Bypass geschaltet sind
- Msec – Aktuelle Bearbeitungszeit der Safety Matrix inklusive F-Kanaltreiber im hierarchischen Plan der Kanaltreiber ("MatrixName")
- MaxMsec – Maximale Bearbeitungszeit der Safety Matrix inklusive F-Kanaltreiber im hierarchischen Plan der Kanaltreiber ("MatrixName"). Dieser Ausgang wird bei jedem Anlauf der Safety Matrix wieder auf 0 zurückgesetzt.

Die unsichtbaren Plananschlüsse (Eingänge und Ausgänge) dürfen nicht verändert werden.

---

**Hinweis**

Nach dem Transfer der Safety Matrix in das Projekt kann mit der Funktion **Extras > Vergleiche Matrix mit > Programm** geprüft werden, ob die Projektkonfiguration mit der Safety Matrix übereinstimmt.

---




**Hierarchischer Plan der Matrixlogik**

Sie dürfen den hierarchischen Plan der Matrixlogik ("@MatrixName") nicht umbenennen, löschen, kopieren oder verschieben.

Sie dürfen nur sichtbare Parameter ändern, nicht jedoch den Parameter "MatrixSig".




**Safety Matrix-Basisplan**

Sie dürfen den Namen des Safety Matrix-Basisplans (im *SIMATIC Manager* sichtbar) nicht ändern.

## 6.2 F-Ablaufgruppe und Ablaufreihenfolge

### Ablaufguppen nach Transfer

Beim Transfer der Safety Matrix in das Projekt werden zwei bzw. drei Ablaufgruppen erstellt:

- Die F-Bausteine aller Matrizen werden in die gemeinsame F-Ablaufgruppe "SafetyMatrixXX" positioniert, wobei "XX" für die Nummer des vorher festgelegten OBs steht. Diese F-Ablaufgruppe beinhaltet den transferierten Code. Sie dürfen hier keine Änderungen vornehmen.

  ---

  **Hinweis**

  Stellen Sie sicher, dass diese F-Ablaufgruppe auch nicht durch die *CFC*-Funktion "Ablaufreihenfolge optimieren" verändert wird. Dies ist gewährleistet, wenn im Eigenschaftsdialog dieser F-Ablaufgruppe das Kontrollkästchen "Optimierung Ablaufreihenfolge" deaktiviert ist.

  ---

- Für alle Safety Matrizen wird eine Standard-Ablaufgruppe "m_SafetyMatrixXX" des jeweiligen OBs erstellt, in der die Standard-Bausteine platziert werden.
- Für jede Safety Matrix, die eigene F-Kanaltreiber besitzt, wird eine Standard-Ablaufgruppe "@Matrixname" angelegt.

#### Ablauffähige Reihenfolge

Bei jedem Transfer der Safety Matrix wird automatisch eine ablauffähige Reihenfolge innerhalb der F-Ablaufgruppe sichergestellt. Die Ablaufreihenfolge orientiert sich am Datenfluss. Falls die Ablaufreihenfolge verfälscht worden sein sollte (z. B. durch einen fehlerhaften Benutzereingriff), so wird diese beim nächsten Transfer automatisch korrigiert und wieder eine ablauffähige Reihenfolge hergestellt.

Diese Reihenfolge hat folgenden systematischen Aufbau:

**Ablaufreihenfolge (mit Vorverarbeitung)**

1. Eingangskanaltreiber
2. Vorverarbeitung
3. F-Bausteine der Safety Matrix
4. Ausgangskanaltreiber

Stellen Sie sicher, dass die Ablaufreihenfolge der in der Vorverarbeitung verwendeten Bausteine korrekt ist.

---

**Hinweis**

Sie dürfen die Reihenfolge der Safety Matrix-Ablaufgruppen nicht ändern.

Sie dürfen die Reihenfolge der Bausteine in den Safety Matrix-Ablaufgruppen nicht ändern.

Die Nichtbeachtung dieses Hinweises führt zu einem F-STOP oder zu einer Reaktion Ihres Sicherheitsprogramms in späterem Zyklus.

---

## 6.3 Hinweise für die Arbeit mit CFC

F-Bausteine sind im *CFC*-Plan farblich gekennzeichnet. Sie sind gelb gefärbt, um Sie darauf aufmerksam zu machen, dass es sich um ein Sicherheitsprogramm handelt.

Die *CFC*-Pläne und F-Ablaufgruppen mit F-Bausteinen sind gelb und mit einem "**F**" markiert, um sie von den Plänen und Ablaufgruppen des Standard-Anwenderprogramms zu unterscheiden.

### Länge des Code-Bereiches optimieren

Falls Sie beim Übersetzen in *CFC* folgende Fehlermeldung erhalten:

```
F: Die maximale Länge des Code-Bereichs (max. 64 Kbyte) ist erreicht.
```

müssen Sie die Größe der F-Ablaufgruppe der Safety Matrix verringern. Hierzu stehen Ihnen verschiedene Projektierungsmöglichkeiten zur Verfügung:

- Verschieben Sie jede Safety Matrix in eine eigene F-Ablaufgruppe.

  Gehen Sie dazu folgendermaßen vor: Verschieben Sie in der Ablaufsicht des *CFC* alle Bausteine eines Safety Matrix-Basisplans in eine neu angelegte F-Ablaufgruppe. Der neuen F-Ablaufgruppe können Sie z. B. den Namen der Safety Matrix als Name vergeben.
- Falls dies nicht ausreichen sollte, teilen Sie (wenn möglich) Ihre große Safety Matrix in mehrere kleinere Safety Matrizen auf.

Wir empfehlen grundsätzlich, große Safety Matrizen in eigene F-Ablaufgruppen zu verschieben. Deren F-Kanaltreiber sollten vor dem Transfer angelegt (z. B. mit Hilfe des IEA) und über die Transfer-Option "Importierte Kanaltreiber verwenden (IEA Unterstützung)" eingebunden werden.

Die Position der Vorverarbeitung kann verändert werden, wenn sie nicht Bestandteil der Safety Matrix-Ablaufgruppe ist (z. B. bei IEA Unterstützung oder kundenspezifischen Kanaltreibern).

### Automatisch erzeugte Pläne

Der Safety Matrix-Plan ist ein automatisch angelegter Plan.

Diesen Plan und die hierarchischen Pläne der folgenden Tabelle (und die wiederum darin enthaltenen hierarchischen Pläne) dürfen Sie nicht umbenennen, verschieben oder löschen.

| Bezeichnung | Name im Projekt |
|---|---|
| Hierarchischer Plan der Matrix | @MatrixName |
| Hierarchischer Plan der Kanaltreiber | MatrixName |
| Hierarchischer Plan der Alarmbausteine (global) | AL_Chart |
| Hierarchischer Plan der Vorverarbeitung | PP_Chart |

# Übersetzen und Laden 7

## 7.1 Übersetzen und Laden in die F-CPU

### Voraussetzung

Alle Safety Matrizen des zu übersetzenden *S7*-Programms sind bereits erfolgreich transferiert worden.

### Übersetzen des SIMATIC-Projekts

1. Vergewissern Sie sich, dass alle Ein- und Ausgänge der Safety Matrix mit dem Sicherheitsprogramm verschaltet sind.
2. Wählen Sie den Menübefehl **Extras > CFC > Übersetzen**.
3. Aktivieren Sie beim Übersetzen der Safety Matrix die Option "Baugruppentreiber erzeugen" im Dialog "Programm übersetzen".
4. Nach dem erfolgreichen Übersetzen des Projekts kann es in die F-CPU geladen werden

#### Laden des SIMATIC-Projekts in die F-CPU

Wählen Sie den Menübefehl **Extras > CPU > Laden**.

Die Matrixlogik kann nun auf ihre einwandfreie Funktion überprüft werden.

# 7.2 Übersetzen und Laden in die Operator Station

## Voraussetzung

Voraussetzung für das Übersetzen und Laden in die Operator Station ist, dass bei der Installation des *Safety Matrix Engineering Tools* V6.2 das Kontrollkästchen für "AS-OS-Engineering" aktiviert ist. Dann ist eine eindeutige Zuordnung der *WinCC*-Bildbausteine zu den Matrizen aus der ES gewährleistet. Siehe Kapitel " Installieren (Seite 24) ".

## Projektierung und Datenablage

Die Projektierung wird in *PCS 7* ausschließlich im ES durchgeführt und anschließend auf die OS-Server geladen. Alle Projektierungsdaten werden zentral verwaltet und im *PCS 7*-Projekt abgelegt. Projektdaten wie Bilder, Variablen und Archive werden auf dem OS-Server abgelegt und für die OS-Clients bereitgestellt.

Der OS-Server wird an den Anlagenbus angeschlossen und verarbeitet die Prozessdaten. Die Bedienung im Prozessbetrieb erfolgt auf den OS-Clients.

---

**Hinweis**

Vor dem Übersetzen und Laden in die OS müssen Sie den beim Transfer der Safety Matrix erzeugten *CFC*-Plan der Safety Matrix in der Technologischen Hierarchie (TH) dem gewünschten Hierarchieordner zuordnen. (Siehe Projektierungshandbuch "Prozessleitsystem PCS7 Engineering System (http://support.automation.siemens.com/WW/view/de/27002758)", Kap. 7.5.10.)

---

## Übersetzen und Laden in die OS

Das Laden eines Projektes wird im *SIMATIC Manager* über die zentrale Funktion "Objekte übersetzen und laden" durchgeführt. Die Darstellung der Objekte in diesem Dialogfeld entspricht der Komponentensicht im *SIMATIC Manager*, d. h. dort werden Ihnen auch alle SIMATIC PC-Stationen angezeigt, die Sie im *SIMATIC Manager* angelegt haben. Hier nehmen Sie zentral alle erforderlichen Einstellungen zum Übersetzen und Laden vor. Zusätzlich legen Sie in diesem Dialogfeld fest, ob Sie das gesamte Projekt oder einzelne Operator Stationen übersetzen und laden möchten.

---

**Hinweis**

Auf einer Single OS wird das OS Übersetzen bei aktivierter *WinCC*-Runtime mit anschließendem Laden nicht unterstützt.

---

## Änderungen einer Safety Matrix übertragen

Änderungen einer Safety Matrix werden nicht automatisch in die Operator Station übernommen. Die Änderungen können Sie mit Übersetzen und Laden in die Operator Station übertragen.

Im Online-Betrieb werden die Abweichungen zwischen Operator Station und F-CPU als roter Text unterhalb der Steuerleiste signalisiert:

- Versionsabweichung
- Matrix-Abweichung

## Besonderheit beim Laden bei Einplatzsystemen

Wenn die OS und das ES auf einem Rechner betrieben werden, müssen Sie keinen Ladevorgang durchführen, weil bereits alle erforderlichen Daten vorhanden sind.

## Siehe auch

Ausführliche Informationen zum Thema "OS übersetzen/laden" finden Sie im Projektierungshandbuch "Prozessleitsystem PCS 7 Operator Station (http://support.automation.siemens.com/WW/view/de/24450116)".

# 8 Bedienen und Beobachten

## 8.1 Übersicht zum Bedienen und Beobachten

### Einleitung

Mit der Funktionalität "Bedienen und Beobachten" der Safety Matrix können Sie das Verhalten einer Safety Matrix im laufenden Betrieb beobachten und bedienen. Dies können Sie sowohl im Online-Betrieb des Engineering Tools als auch mit dem Viewer von einer PCS7 OS aus durchführen.

### Voraussetzungen für das Bedienen und Beobachten

Bedienen und Beobachten an der Engineering Station führen Sie im Online-Betrieb des *Safety Matrix Engineering Tools* durch.

Bedienen und Beobachten an der Operator Station führen Sie über den Bildbaustein *Safety Matrix Viewer* durch.

Es gelten die folgenden Voraussetzungen für das Bedienen und Beobachten einer Safety Matrix.

### An der ES (Safety Matrix Engineering Tool)

- Eine Safety Matrix ist erstellt und in das Projekt transferiert.
- Das *S7*-Programm mit der Safety Matrix ist übersetzt und in die F-CPU geladen.
- Zum Bedienen: Der Eingang EN_SWC des hierarchischen Plans der Matrixlogik ("@MatrixName") zur Freigabe von Secure Write ist auf TRUE gesetzt.

### An der OS (Safety Matrix Viewer)

- Das *S7*-Programm mit der Safety Matrix ist übersetzt und in die F-CPU geladen.
- Der/die Benutzer mit den entsprechenden Berechtigungen sind eingerichtet.
- Die Projektierung der Safety Matrix-Bildbausteine ist in die OS geladen.
- Zum Bedienen: Der Eingang EN_SWC des hierarchischen Plans der Matrixlogik ("@MatrixName") zur Freigabe von Secure Write ist auf TRUE gesetzt.
- Beim Einsatz von OS-Clients müssen Sie sicherstellen, dass für Variablen kein Standardserver eingestellt ist (im *WinCC*-Explorer "Serverdata" markieren, aus dem Kontextmenü "Standardserver" wählen und im Dialog "Standardserver konfigurieren" für die Komponente "Variablen" "kein Standardserver" einstellen).

## Unterschiede beim Bedienen und Beobachten zwischen ES und OS

| ES (*Safety Matrix Engineering Tool*) | OS (*Safety Matrix Viewer*) |
|---|---|
| Steuerleiste | Steuerleiste<br>• ohne Steuerleistenfunktion Bypass-Report |
| Bedienung der Safety Matrix mittels Secure Write-Transaktion im Online-Betrieb | Bedienung der Safety Matrix mittels Secure Write-Transaktion über Bildbaustein |
| - | Zusätzlich werden die Benutzerberechtigungen und das 2-Bediener-Szenario unterstützt |
| Bedienungen, die die Signatur des Programms verändern (Werte für zulässige Diskrepanz (Delta), Limit und Hysterese) | - |
| Parametrierung von oberen und unteren Bereichsgrenzen an F-Kanaltreibern für analoge TAGs | - |
| Kontextmenüs vorhanden | - |
| Ereignisse und Meldungen<br>• Ereignisprotokoll (Event Log) | Ereignisse und Meldungen<br>• Ereignisprotokoll (Event Log)<br>• *PCS 7*-Alarm- und Bedienmeldungen im Meldearchiv |

⚠ WARNUNG

**Warn- und Sicherheitshinweise des Benutzerhandbuchs zur *Safety Matrix* V5.2**

Wenn Sie die Safety Matrix noch nicht mit dem *Safety Matrix Engineering Tool* ab V 6.1 transferiert haben, müssen Sie sämtliche Warn- und Sicherheitshinweise des Benutzerhandbuchs zur *Safety Matrix* V5.2 beachten. (Siehe Benutzerhandbuch "Safety Matrix (http://support.automation.siemens.com/WW/view/de/31609780)".)

⚠ WARNUNG

**Unabhängige Wege zur Anzeige**

Zum Einleiten sicherheitskritischer Aktionen, z. B. Bedienungen, müssen Sie Anzeigen auf voneinander unabhängigen Wegen nutzen. Die Safety Matrix bietet Ihnen dazu die Statusanzeigen und das Ereignisprotokoll. Die verschiedenen Arten der Statusanzeige sind nicht voneinander unabhängig, auch nicht die Anzeigen im Online-Betrieb des *Safety Matrix Engineering Tools* und die Anzeigen im *Safety Matrix Viewer*.

## 8.2 Starten des Online-Betriebs im Engineering Tool

### Einleitung

Der Online-Betrieb im *Safety Matrix Engineering Tool* ermöglicht die Beobachtung des Status einer Safety Matrix, die in die F-CPU geladen wurde.

### Starten und Beenden des Online-Betriebs

Zum Starten/Beenden des Online-Betriebs wählen Sie den Menübefehl **Beobachten > Beobachten Ein/Aus**.

Das *Safety Matrix Engineering Tool* stellt die Verbindung zur Safety Matrix in der F-CPU her. Nachdem die Verbindung aufgebaut ist, wird der aktuelle Status der Causes und Effects angezeigt.

## 8.3 Öffnen der Safety Matrix Viewer-Bildbausteine

### Einleitung

Während der Laufzeit können Sie den *Safety Matrix Viewer* aus *WinCC* heraus starten. Der *Safety Matrix Viewer* bietet eine visuelle Darstellung der Safety Matrix, so wie sie im *Safety Matrix Engineering Tool* projektiert ist und überwacht wird.

Der *Safety Matrix Viewer* zeigt die gesamte Konfiguration einer Safety Matrix an (mit Causes, Effects und Schnittpunkten), die Projektierung kann nicht geändert werden.

Der *Safety Matrix Viewer* ermöglicht das gleichzeitige Bedienen und Beobachten mehrerer Matrizen. Außerdem unterstützt der *Safety Matrix Viewer* die gleichzeitige Überwachung einer Safety Matrix auf mehreren Client-Stationen.

---

**Hinweis**

Bei einem *WinCC*-Benutzerwechsel wird der aktuell geöffnete Safety Matrix-Bildbaustein automatisch geschlossen und kann anschließend nur mit den neuen Berechtigungen des neuen Benutzers geöffnet werden. Falls der Safety Matrix-Bildbaustein während eines *WinCC*-Benutzerwechsels geöffnet ist, z. B. wegen Änderungen von *WinCC*-Skripten, muss der Safety Matrix-Bildbaustein manuell geschlossen werden, bevor sich der neue Benutzer anmeldet.

---

**Hinweis**

Sollen beim anschließenden OS Übersetzen eines bestehenden Bildes die vom Anwender vergebenen Einstellungen am Bausteinsymbol einer Safety Matrix beibehalten werden, so deaktivieren Sie für dieses *WinCC*-Bild die Option "Bausteinsymbole aus der Technologischen Hierarchie ableiten".

---

## Voraussetzung für das Erzeugen von Bausteinsymbolen

Voraussetzung für das Erzeugen der im Folgenden beschriebenen Bausteinsymbole für die Safety Matrix ist die entsprechende Projektierung der Meldebausteine (siehe Kapitel "Meldungsprojektierung (Seite 61)") und der Transfer der Safety Matrix mit aktivierter Option "Alarm-Bausteine platzieren" (siehe Kapitel "Transferieren der Safety Matrix in das Projekt (Seite 111)").

## Öffnen des Safety Matrix Viewer

1. Melden Sie sich an der OS als Benutzer mit den erforderlichen Berechtigungen an.
2. Öffnen Sie das Bild, in dem die gewünschten Safety Matrix-Bausteinsymbole enthalten sind. Beim OS Übersetzen der Safety Matrix werden für die projektierten Meldebausteine F_MA_AL (Safety Matrix, 1-mal), F_SC_AL (Causes, x-mal) und F_SE_AL (Effects, x-mal) die entsprechenden Bausteinsymbole erzeugt. Diese bieten unterschiedliche Sichten, nämlich:
   – auf die gesamte Safety Matrix
   – auf einen einzelnen Cause mit zugehörigen Schnittpunkten und Effects
   – auf einen einzelnen Effect mit zugehörigen Schnittpunkten und Causes
3. Klicken Sie auf das jeweilige Bausteinsymbol, um den *Safety Matrix Viewer*-Bildbaustein mit der gewünschten Sicht zu öffnen.

## Safety Matrix-Bausteinsymbol




Das Safety Matrix-Bausteinsymbol zeigt die folgenden Angaben für die Safety Matrix:

- Technologischer Name des Safety Matrix-Meldebausteins
- Anzeige, ob aktive Vorwarnungen für Causes anstehen
- Anzeige, ob aktive Vorwarnungen für Effects anstehen
- Anzeige, ob aktive Causes anstehen
- Anzeige, ob aktive Effects anstehen
- Anzahl der aktiven Causes
- Anzahl der aktiven Effects
- Anzeige, ob Causes mit Bypass anstehen
- Anzeige, ob Effects mit Bypass anstehen
- Anzahl der Causes mit Bypass
- Anzahl der Effects mit Bypass
- Text zu Filterung der Anzeige auf eine SIF-Gruppe (falls projektiert)
- Nummer der SIF-Gruppe (falls projektiert)
- Anzeige, ob die Konfiguration geändert wurde
- Anzeige, ob Wiedereingliederung der F-Kanaltreiber erforderlich ist.

### Attribute für das Filtern der Anzeige der Safety Matrix

Mit dem Attribut "SafetyGroupNumber" in der Eigenschaft "MatrixData" geben Sie die Nummer derjenigen Sicherheitstechnischen Funktionsgruppe (SIF-Gruppe) ein, deren zugeordnete Causes und Effects beim Öffnen des Safety Matrix-Bildbausteins angezeigt werden sollen. Alle anderen Causes und Effects werden dann ausgeblendet, auch solche, die keiner SIF-Gruppe zugeordnet sind.

Damit Sie am Bausteinsymbol erkennen können, ob die Safety Matrix gefiltert angezeigt wird, können Sie am Attribut "SafetyGroupDescription" einen Text angeben. Dieser Text wird in der dritten Zeile des Bausteinsymbols ausgegeben, die ansonsten leer bleibt.

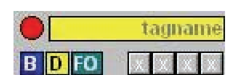
Die folgende Tabelle gibt einen Überblick über die Eigenschaften für die Filterung:

| Bezeichnung in Eigenschaft "MatrixData" | Beschreibung | Voreinstellung |
|---|---|---|
| SafetyGroupNumber | numerische Voreinstellung der SIF-Gruppe in der Safety Matrix | 0 (= alle Causes und Effects werden angezeigt) |
| SafetyGroupDescription | textuelle Voreinstellung der SIF-Gruppe in der Safety Matrix | - |

### Attribute für das Einstellen der Farben der Anzeigen

Das Bausteinsymbol bietet Ihnen die Möglichkeit, mittels Attributen die Hintergrund- und Schriftfarbe der Anzeigen zu ändern.

## Cause-Bausteinsymbol




Das Cause-Bausteinsymbol zeigt die folgenden Angaben für einen Cause:

- Technologischer Name des Cause-Meldebausteins
- Anzeige, ob der Cause aktiv ist (roter Kreis)
- Anzeige, ob es eine Vorwarnung für den Cause gibt (gelber Kreis)
- Anzeige, ob es einen Bypass für den Cause gibt
- Anzeige, ob es einen Diagnosealarm/Fehler für den Cause gibt
- Anzeige, ob Quittierung des First Out-Alarms erforderlich ist.

### Attribute für das Einstellen der Farben der Anzeigen

Das Bausteinsymbol bietet Ihnen die Möglichkeit, mittels Attributen die Hintergrund- und Schriftfarbe der Anzeigen zu ändern.

## Effect-Bausteinsymbol




Das Effect-Bausteinsymbol zeigt die folgenden Angaben für einen Effect:

- Technologischer Name des Effect-Meldebausteins
- Anzeige, ob der Effect aktiv ist (roter Kreis)
- Anzeige, ob es eine Vorwarnung für den Effect gibt (gelber Kreis)
- Anzeige, ob es einen Bypass für den Effect gibt
- Anzeige, ob es einen Diagnosealarm/Fehler für den Effect gibt
- Anzeige, ob Rücksetzen möglich ist.

### Attribute für das Einstellen der Farben der Anzeigen

Das Bausteinsymbol bietet Ihnen die Möglichkeit, mittels Attributen die Hintergrund- und Schriftfarbe der Anzeigen zu ändern.

## Berechtigung für Sammelquittierung an den Bausteinsymbolen

Ab V6.2 gibt es an den Bausteinsymbolen der Safety Matrix eine Berechtigung für die Sammelquittierung von Alarmen und Meldungen. Klicken Sie mit der rechten Maustaste auf das jeweilige Bausteinsymbol und wählen Sie unter der Eigenschaft "Sonstige" die Berechtigung "Processcontrolling_backup" aus, um die Berechtigungsstufe festzulegen.

# 8.4 Beobachten

## 8.4.1 Farbcodes zur Statusanzeige

### Farben

Im Online-Betrieb der Safety Matrix wird der Status von Causes, Schnittpunkten und Effects mit verschiedenen Farben angezeigt. Diese Farben sind voreingestellt und können geändert werden (siehe Kapitel "Die Dialoge "Anpassen" (Seite 80)").

## 8.4.2 Statusanzeigen

### Beobachtungsfunktion "Status anzeigen" in der Steuerleiste

Die Schaltfläche **Status anzeigen** ist verfügbar, wenn ein Cause oder ein Effect ausgewählt ist. Durch Klicken auf diese Schaltfläche wird das Anzeigefenster "Cause-Status" oder "Effect-Status" geöffnet. Diese Anzeigefenster enthalten Informationen für den ausgewählten Cause oder Effect.

Ist ein Status weiß hinterlegt, so ist er aktiv.

### Statusbeschreibungen Cause

| Cause-Status | Beschreibung | Eintrag im Ereignis-protokoll |
|---|---|---|
| Cause aktiv | Zeigt an, dass alle projektierten Kriterien für den aktiven Zustand erfüllt sind (Status, Funktionslogik, Zeitverzögerungen usw.). | X |
| Zeitsteuerung aktiv | Zeigt an, dass eine projektierte Zeitsteuerung aktiv ist. Nach Ablauf der Zeitdauer wird Bit "aktiv" gelöscht. | |
| Hysterese aktiv | Zeigt an, dass ein aktiver Cause seine Auslösebedingung verlassen hat, aber immer noch innerhalb der projektierten Totzone ist. | |
| Unterdrückung aktiv | Zeigt an, dass der Unterdrücken-TAG aktiv ist. | X |
| Bypass aktiv | Zeigt an, dass ein Bypass aktiv ist. | X |
| Soft-Bypass aktiv | Zeigt an, dass der aktuelle Bypass über eine Bedienung gesetzt wurde. | X |
| Auslösung angefordert | Zeigt an, dass die Verknüpfung der TAGs entsprechend der Funktionslogik erfüllt ist. Der aktive Status des Cause kann durch das projektierte Zeitverhalten oder Bypass, Unterdrückung, Verriegelung beeinflusst sein. | |
| Diskrepanzfehler (TAG X –TAG Y) | Zeigt an, dass die berechnete TAG-Differenz (X - Y) den projektierten Delta-Alarmwert überschritten hat. | |

| Cause-Status | Beschreibung | Eintrag im Ereignis-protokoll |
|---|---|---|
| Alarm Auslösung Input | Bei einem Cause mit mehreren TAGs zeigt dieser Status an, dass mindestens ein TAG die Auslösebedingung erreicht hat und eine Auslösung anfordert, diese aber nicht aktiv geworden ist. | |
| Konfigurationsfehler | Fehler bei interner Diagnoseprüfung des FB (interner Fehler; Abhilfe: ggf. neu transferieren, übersetzen und laden). | |
| SDF-Fehler | Zeigt an, dass die Safety Matrix einen Fehler im Sicherheitsdatenformat im DB erkannt hat. Dieser Fehler führt immer zu einem F-STOP im Sicherheitsprogramm. | X |
| Quitt. Cause erforderlich | Zeigt an, dass der Cause im aktiven Zustand gehalten wird, bis er vom Anwender quittiert wird und die Auslösebedingung nicht mehr erfüllt ist. | X |
| TAG x Auslösung Vorwarnung | Zeigt an, dass der projektierte TAG die Bedingung für die Limit-Vorwarnung erfüllt. | X |
| TAG x Auslösung angefordert | Zeigt an, dass der projektierte TAG die Bedingung für die Anforderung einer Auslösung erfüllt. Dieser Status beinhaltet die Energize-to-trip-Einstellung des TAG. | X |
| TAG x Wert | Zeigt den TAG-Status an. | |
| TAG x Bad Quality | Zeigt an, dass der F-Kanaltreiber des projektierten TAG einen Qualitätsalarm meldet. | X |
| TAG x simuliert | Zeigt an, dass der TAG simuliert wird. | X |
| TAG x Kanalfehler | Zeigt an, dass der F-Kanaltreiber des projektierten TAG einen Kanalfehler meldet. | X |
| TAG x PROFIsafe-Fehler | Zeigt an, dass der F-Kanaltreiber des projektierten TAG einen PROFIBUS-Fehler meldet, dessen Ursache der Baugruppentreiber ist. | X |

## Statusbeschreibungen Effect

| Effect-Status | Beschreibung | Eintrag im Ereignis-protokoll |
|---|---|---|
| Effect aktiv | Zeigt an, dass alle projektierten Kriterien für den aktiven Zustand erfüllt sind (Schnittpunktstatus, Bypass usw.). | X |
| Verzögerung aktiv | Zeigt an, dass eine Zeitverzögerung aktiv ist. | |
| Maskierung aktiv | Zeigt an, dass eine Maskierung aktiv ist. | X |
| Übersteuern aktiv | Zeigt an, dass eine Übersteuern-Funktion aktiv ist. | X |
| N Schnittpunkte | Zeigt an, dass ein verschalteter Schnittpunkttyp N aktiv ist. | |
| S Schnittpunkte | Zeigt an, dass ein verschalteter Schnittpunkttyp S aktiv ist. | |
| V Schnittpunkte | Zeigt an, dass ein verschalteter Schnittpunkttyp V aktiv ist. | |
| R Schnittpunkte | Zeigt an, dass ein verschalteter Schnittpunkttyp R aktiv ist. | |

| Effect-Status | Beschreibung | Eintrag im Ereignis-protokoll |
|---|---|---|
| Bypass aktiv | Zeigt an, dass ein Bypass aktiv ist. | X |
| Soft-Bypass aktiv | Zeigt an, dass der aktuelle Bypass über eine Bedienung gesetzt wurde. | X |
| Durchreichen aktiv | Zeigt an, dass in der Effect-Logik "Prozesswert durchreichen" aktiv ist. | X |
| Übersteuern Input | Zeigt an, dass der Effect aktuell übersteuert wird. | |
| OK zum Übersteuern | Zeigt an, dass der Effect bereit zum Übersteuern ist. | |
| OK zum Rücksetzen | Zeigt an, dass der Effect bereit zum Rücksetzen ist. | |
| Effect gespeichert | Zeigt an, dass der Effect gespeichert ist und rückgesetzt werden muss. | X |
| Übersteuern Vorwarnung | Zeigt an, dass der Effect die Bedingung Zeit-Vorwarnung für die max. Übersteuern-Zeit erfüllt. | X |
| Fehler Überst.: Cause | Zeigt an, dass das Übersteuern des Effect unterbrochen wurde, weil ein neuer Cause aktiv wurde. | |
| Fehler Überst.: Zeitüber. | Zeigt eine Zeitüberschreitung beim Übersteuern des Effect an. | |
| Konfigurationsfehler | Fehler bei interner Diagnoseprüfung des FB (interner Fehler; Abhilfe: ggf. neu transferieren, übersetzen und laden). | |
| SDF-Fehler | Zeigt an, dass die Safety Matrix einen Fehler im Sicherheitsdatenformat im DB erkannt hat. Dieser Fehler führt immer zu einem F-STOP im Sicherheitsprogramm. | X |
| TAG x Wert | Zeigt den aktuellen Status des Output-TAG an. | |
| TAG x Bad Quality | Zeigt an, dass der F-Kanaltreiber des projektierten TAG einen Qualitätsalarm meldet. | X |
| TAG x simuliert | Zeigt an, dass der TAG simuliert ist. | X |
| TAG x Kanalfehler | Zeigt an, dass der F-Kanaltreiber des projektierten TAG einen Kanalfehler meldet. | X |
| TAG x PROFIsafe-Fehler | Zeigt an, dass der F-Kanaltreiber des projektierten TAG einen PROFIBUS-Fehler meldet, dessen Ursache der Baugruppentreiber ist. | X |
| Effect übersteuern: Restzeit | Zeigt die Restzeit an, die der Effect noch übersteuert werden kann. | |

# 8.5 Bedienen

Während im Online-Betrieb des *Safety Matrix Engineering Tools* nach Eingabe des Passworts für das Sicherheitsprogramm sämtliche Steuerleistenfunktionen uneingeschränkt zur Verfügung stehen, sind die verfügbaren Funktionen im *Safety Matrix Viewer* an der PCS 7 OS abhängig von der Zuordnung der Funktionen zu einer Berechtigungsstufe am Bausteinsymbol und den entsprechend projektierten Benutzerberechtigungen in der PCS 7 OS.




**Standard-Bediener**

Stellen Sie sicher, dass ein Standard-Bediener, z. B. Autologin, keine Bedienberechtigung für die Safety Matrix zugewiesen bekommt.

## 8.5.1 Initiator- und Confirmer-Berechtigung

### 2-Bediener-Szenario

Bei der Projektierung der Safety Matrix in der PCS 7 OS können Sie ein 2-Bediener-Szenario wählen (4-Augen-Prinzip). Hierfür sind zwei Rollen für Bediener definiert: Initiator und Confirmer. Mit den entsprechenden Attributen "Initiator" bzw. "Confirmer" legen Sie fest, welche Berechtigung der Bediener der PCS 7 OS besitzen muss, um als Initiator oder als Confirmer die Bedienfunktionen am *Safety Matrix Viewer* durchführen zu können:

- Initiator-Berechtigung: Der Bediener darf eine Bedienung starten.
- Confirmer-Berechtigung: Der Bediener darf eine Bedienung bestätigen.

Sind die Confirmer-Berechtigung und die Initiator-Berechtigung auf 0 gesetzt (= kein Zugriffschutz), so wird das 2-Bediener-Szenario nicht verwendet. Die Bedienung der einzelnen Funktionen ist dann allein abhängig von der für die jeweilige Bedienfunktion festgelegten Berechtigungsstufe.

Die Benutzer müssen zusätzlich zu der Initiator- und/oder Confirmer-Berechtigung die festgelegte Berechtigungsstufe für die jeweils auszuführende Bedienfunktion besitzen.

### Vorgehensweise

Sie projektieren die Zuordnung der Funktionen der Safety Matrix zu einer Berechtigungsstufe in der PCS 7 OS im Dialog "Eigenschaften" der Safety Matrix, Register "Berechtigungen OS" (siehe Kapitel "Der Dialog "Eigenschaften" der Safety Matrix (Seite 75)").

## Benutzerberechtigungen für Bediener einrichten

Abhängig davon, ob die Transaktion von zwei Bedienern oder nur von einem Bediener durchgeführt wird, legen Sie folgende Benutzer an.

### Bedienung mit zwei Bedienern

Wenn die Transaktion für die Bedienung einer Safety Matrix von zwei Bedienern durchgeführt wird, legen Sie zwei Benutzer an:

- Der Initiator startet die Bedienung einer Safety Matrix über Secure Write. Dieser Benutzer muss die Berechtigung besitzen, die dem Attribut "Initiator" in den Eigenschaften der Safety Matrix zugewiesen ist. Der Initiator besitzt jedoch nicht die Berechtigung, die Bedienung zu bestätigen.
- Der Confirmer überprüft und bestätigt die Bedienung. Dieser Benutzer muss die Berechtigung besitzen, die dem Attribut "Confirmer" in den Eigenschaften der Safety Matrix zugewiesen ist. Der Confirmer besitzt jedoch nicht die Berechtigung, die Bedienung zu starten.

### Bedienung mit einem Bediener

- Wenn alle Schritte der Transaktion von nur einem Bediener, aber mit Initiator/Confirmer-Zugriffschutz durchgeführt werden, legen Sie einen Benutzer an, der beide Berechtigungen besitzt, die den Attributen "Initiator" und "Confirmer" in den Eigenschaften der Safety Matrix zugewiesen sind.

Die Benutzer und eigene Berechtigungsstufen legen Sie in der PCS 7 OS mit dem Editor "User Administrator" an.

## OS aktivieren

Aktivieren Sie das Runtime-System der PCS 7 OS, z. B. im *WinCC*-Explorer mit dem Menübefehl **Datei > Aktivieren**.

Nach erfolgtem Aktivieren erscheinen die Hierarchieebenen als Schaltflächen im Runtime-System der OS. Durch Betätigen der Schaltfläche werden die Bausteinsymbole dieser Ebene angezeigt.

## OS deaktivieren

Schließen Sie den *Safety Matrix Viewer*, bevor Sie das Runtime-System der OS deaktivieren.

## Siehe auch

Kapitel "Transaktion für Secure Write (Seite 136)"

## 8.5.2 Secure Write

### 8.5.2.1 Transaktion für Secure Write

#### Was ist eine Transaktion für Secure Write?

Eine Transaktion zur Bedienung einer Safety Matrix über Secure Write führen Sie im Online-Betrieb des Engineering Tools bzw. in der OS über den Safety Matrix-Bildbaustein durch. Die Transaktion besteht aus einer Bedienfolge, die von einem oder zwei Bedienern durchgeführt werden kann.

Die Transaktion muss innerhalb eines vom Anwender festzulegenden Zeitintervalls abgeschlossen sein (Timeout). Wenn die Transaktion nicht innerhalb dieses Zeitintervalls beendet wird, wird sie automatisch abgebrochen.

#### Voraussetzungen

- Das Safety Matrix-Programm ist übersetzt und in die F-CPU geladen, und die F-CPU befindet sich im RUN. Siehe Kapitel "Übersetzen und Laden in die F-CPU (Seite 121) ".
- Bei Bedienung über die OS: Die Projektierung der Bildbausteine ist in die OS geladen. Siehe Kapitel "Übersetzen und Laden in die Operator Station (Seite 122) ".
- Der/die Bediener mit den entsprechenden Berechtigungen sind eingerichtet. Siehe Kapitel "Der Dialog "Eigenschaften" der Safety Matrix (Seite 75) ".
- Der Eingang EN_SWC des hierarchischen Plans der Matrixlogik zur Freigabe von Secure Write ist auf TRUE gesetzt und das Zeitintervall ist projektiert. Siehe Kapitel "Der Dialog "Eigenschaften" der Safety Matrix (Seite 75) ".
- Bei Bedienung über die OS müssen Sie das Verlassen der OS-Oberfläche wie in *PCS 7* üblich unterbinden (Tastenkombination sperren).

## Allgemeine Hinweise

**Hinweis**

Im *Safety Matrix Viewer* V6.2 können Sie keine Bedienungen vornehmen, die die Signatur des Sicherheitsprogramms verändern, d. h. die Werte für zulässige Diskrepanz (Delta), Limit und Hysterese können nicht verändert werden. Der entsprechende Dialog ist nur im *Safety Matrix Engineering Tool* verfügbar.

**⚠ WARNUNG**

**Durch die Funktionalität "Secure Write" werden Änderungen im RUN am Sicherheitsprogramm vorgenommen**

Dies macht zusätzliche Sicherheitsmaßnahmen erforderlich:

- Sorgen Sie dafür, dass Änderungen nur dann durchgeführt werden können, wenn dies die Sicherheit der Anlage nicht beeinträchtigt. Dafür können Sie den bereitgestellten Eingang #EN_SWC nutzen, z. B., indem Sie ihn mit einem Schlüsselschalter oder prozessabhängig durch das Sicherheitsprogramm steuern.
- Sorgen Sie dafür, dass nur berechtigte Personen Änderungen durchführen können. Dabei dürfen Sie sich nicht ausschließlich auf die projektierten Berechtigungen im Bausteinsymbol verlassen. Beispiele:
  - Steuern Sie den Eingang EN_SWC mit einem Schlüsselschalter.
  - Richten Sie einen Zugangsschutz zu den Operator Stationen ein, an denen die Funktion "Secure Write" durchgeführt werden kann.



**⚠ WARNUNG**

**Bedienen einer Safety Matrix**

Stellen Sie durch organisatorische Maßnahmen sicher, dass an einer Safety Matrix zu einem Zeitpunkt nur eine Transaktion initiiert bzw. bestätigt werden kann.

**⚠ WARNUNG**

**Secure Write: Korrekte Funktion der Bedienung prüfen**

Sie müssen die korrekte Funktion der Bedienung prüfen. Unmittelbar nach einer Bedienung muss:

- die erwartete Reaktion der Bedienung als Änderung in der Statusanzeige erkennbar sein oder
- der Status zu dieser Bedienung den Einträgen im Ereignisprotokoll entsprechen.

**⚠ WARNUNG**

**Prüfen einer Transaktion**

Als Bediener dürfen Sie nur die erwarteten Angaben akzeptieren. Bei Inkonsistenzen müssen Sie die Transaktion abbrechen. Sie dürfen nur die Ihnen organisatorisch zugeordnete Transaktion bestätigen.

⚠ WARNUNG

**Prüfen der technologischen Zuordnung**

Überprüfen Sie beim Öffnen des Bildbausteins, dass die technologische Zuordnung in der obersten Zeile zum Umfeld passt, in dem das Bausteinsymbol platziert wurde. Somit stellen Sie sicher, dass Sie die richtige Safety Matrix bedienen.

⚠ WARNUNG

**Abbruch einer Transaktion**

Sie müssen immer mit dem Abbruch einer Transaktion durch unvorhergesehene Ereignisse, z. B. Kommunikationsfehler, rechnen, die Sicherheit der Anlage darf dadurch nicht gefährdet werden.

### Bedienerrollen für Secure Write

Eine Transaktion kann durch einen einzelnen Bediener durchgeführt werden, der die Bedienung startet, überprüft und bestätigt. An der OS kann eine Transaktion aber auch durch zwei Bediener durchgeführt werden. Ein Bediener startet die Bedienung (Initiator) und der Zweite überprüft und bestätigt sie (Confirmer).

### Ablauf einer Transaktion für Secure Write

Eine Transaktion besteht aus mehreren Dialogen, die nacheinander bedient werden müssen. Nachdem Sie einen Dialog bedient haben, kann es (abhängig von der Auslastung des Servers oder des Kommunikationskanals zur CPU) zu Wartezeiten kommen, bis sich der Folgedialog öffnet.

Um diesen Vorgang transparenter zu machen, wird am Anfang jeder Transaktion ein Dialog geöffnet, der bis zum Ende der Transaktion geöffnet bleibt. Zusätzlich zeigt Ihnen dieser Dialog weitere Informationen an, wie z. B. die für die Transaktion verbleibende Restzeit und Fehlermeldungen.

### 8.5.2.2 Varianten von Secure Write

#### Welche Varianten von Secure Write gibt es?

Secure Write steht in 3 Varianten zur Verfügung:

- Vollständiges Secure Write (im Online-Betrieb des *Safety Matrix Engineering Tools* bzw. von der PCS 7 OS über den *Safety Matrix Viewer*):
  Der Bediener besitzt sowohl die Initiator- als auch die Confirmer-Berechtigung und kann die Transaktion alleine durchführen.
- Secure Write für Initiator (nur über *Safety Matrix Viewer* an der PCS 7 OS):
  Wenn der Bediener die Initiator-Berechtigung hat, kann er die Transaktion als Initiator starten.
- Secure Write für Confirmer (nur über *Safety Matrix Viewer* an der PCS 7 OS):
  Wenn der Bediener die Confirmer-Berechtigung hat, kann er die Transaktion als Confirmer bestätigen. Erst nach dieser Bestätigung wird die Bedienung im Sicherheitsprogramm wirksam.

## 8.5.3 Bedienung einer Safety Matrix

### 8.5.3.1 Bedienen mit der Steuerleiste im Online-Betrieb und im Safety Matrix Viewer

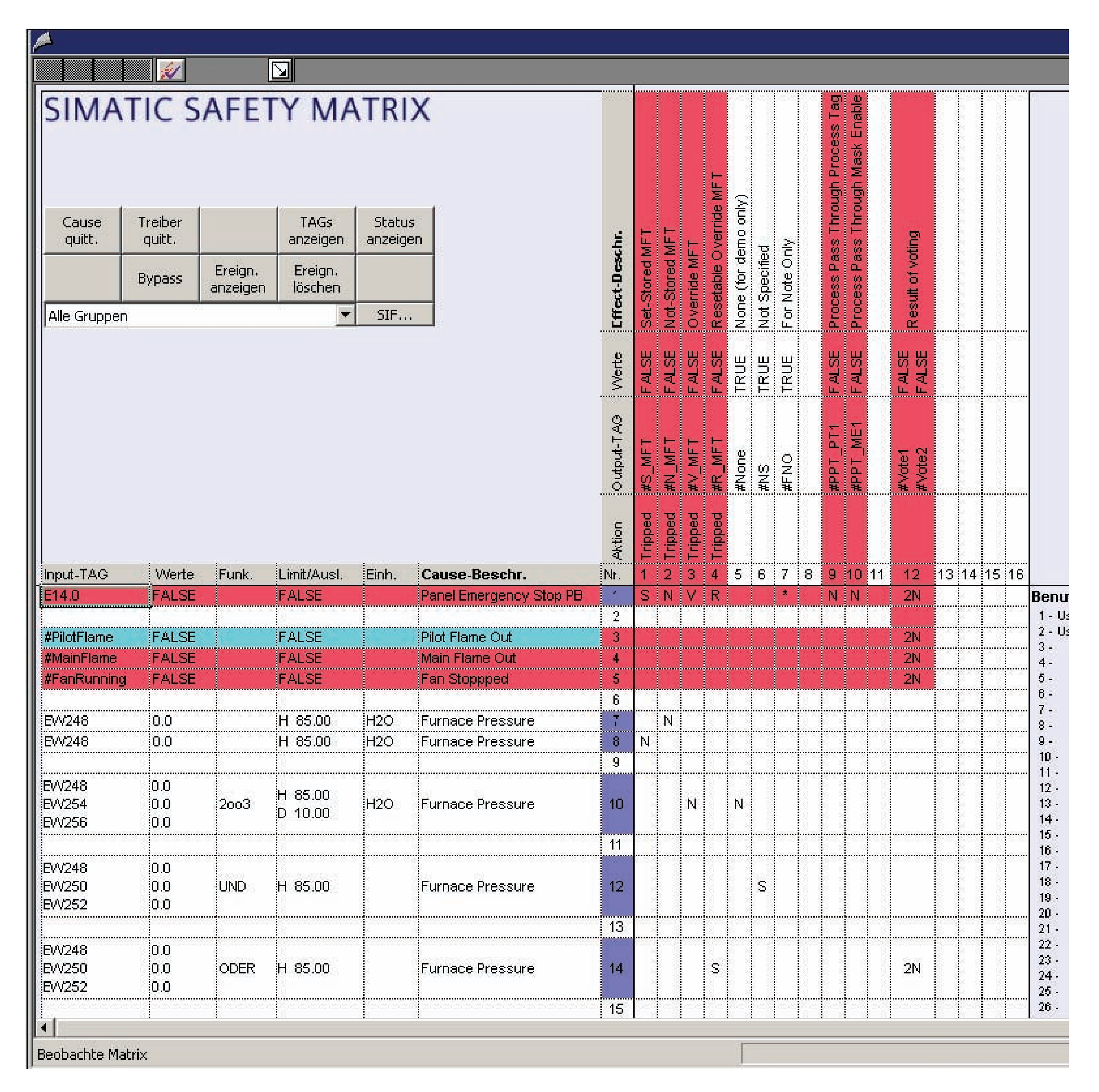
#### Abhängigkeit der verfügbaren Funktionen

Für die Arbeit mit einer Online-Safety Matrix steht im Online-Betrieb des *Safety Matrix Engineering Tools* und im *Safety Matrix Viewer* die Steuerleiste zur Verfügung. Nachdem ein Cause oder ein Effect in der Safety Matrix ausgewählt ist, werden die dafür verfügbaren Steuerleistenfunktionen in den Schaltflächen der Steuerleiste angezeigt. Steuerleistenfunktionen, für die keine Berechtigung vorliegt, werden gegraut dargestellt.

Welche Funktionen jeweils verwendbar sind, hängt ab von:

- dem ausgewählten Element,
- der Konfiguration des Elements
- dem Status des Elements
- der Benutzerberechtigung an der PCS 7 OS

Das folgende Beispiel zeigt die Steuerleiste mit einem hervorgehobenen Cause, der eine Quittierung (ACK) durch den Benutzer erfordert.



## Beschreibung der Steuerleistenfunktionen

| Steuerleistenfunktion | Funktion | Benutzerberechtigung an OS erforderlich |
|---|---|---|
| Ereign. anzeigen | Mit dem Ereignisprotokoll kann die Safety Matrix ereignisbezogene Informationen z. B. anhand von Zustandswechseln von Cause und Effect speichern. Es werden umlaufend maximal 100 Ereignisse protokolliert. Damit ist gewährleistet, dass stets die neueren Ereignisse in der Anzeige stehen.<br>Mit der Funktion "Ereignisse anzeigen" können Ereignisse der Safety Matrix aus der F-CPU gelesen und im Log-Fenster, auch im *Safety Matrix Viewer*, angezeigt werden. Siehe Beschreibung der Statusdetails für Cause und Effect mit Informationen, welche Benutzeraktionen und Diagnoseereignisse aufgezeichnet werden. | - |
| Status anzeigen | Schaltfläche **Status anzeigen** ist verfügbar, wenn ein Cause oder ein Effect ausgewählt ist. Durch Klicken auf diese Schaltfläche wird das Anzeigefenster "Cause-Status" oder "Effect-Status" geöffnet. Diese Anzeigefenster enthalten Informationen für den ausgewählten Cause oder Effect.<br>Siehe Kapitel "Statusanzeigen (Seite 131)". | - |
| TAGs anzeigen | Mit Klick auf Schaltfläche **TAGs anzeigen** wird ein Dialog angezeigt, in dem die Werte von Cause- oder Effect-TAGs betrachtet werden können. Zum Simulieren eines Cause- oder Effect-TAG benötigen Sie jedoch die entsprechende Benutzerberechtigung. | - |
| Cause quitt. | Schaltfläche **Cause quitt.** ist bereit, wenn der ausgewählte Cause aktiv und ohne automatische Quittierung projektiert ist. Es wird eine Quittierungsanforderung angezeigt und der Cause bleibt aktiv, bis die Schaltfläche **Cause quitt.** angeklickt wird und die Auslösebedingungen, die den Cause aktiviert haben, nicht mehr erfüllt sind. | CauseAckLevel |
| First Out löschen | Ein Farbwechsel zeigt an, welcher Cause zuerst die zugehörige First Out Alarm-Gruppe ausgelöst hat. Dieser erste Cause wird in Cyan markiert, bis der Cause und Schaltfläche **First Out löschen** angeklickt werden. | CauseClrFOLevel |
| Bypass | Mit Schaltfläche **Bypass** wird verhindert, dass ein Cause oder ein Effect aktiv wird. Wird ein Cause oder ein Effect mit Bypass umgangen, so wird er nicht aktiv. | CauseBypLevel / EffectBypLevel |
| Ereign. löschen | Funktion "Ereignisse löschen" veranlasst das Löschen des Ereignisprotokolls in der F-CPU. | EventsClearLevel |
| Alarm löschen | Funktion "Alarm löschen" wird aktiv, wenn ein Effect ausgewählt wurde, der übersteuert wurde, aber aus einem der folgenden Gründe erneut aktiv geworden ist:<br>• die projektierte maximale Übersteuern-Zeit ist abgelaufen<br>• sie wurde durch einen neuen aktiven Cause erneut ausgelöst.<br>In diesen Fällen wird der betroffene Effect durch einen Farbwechsel angezeigt. Über die Schaltfläche "Löschen" können Sie den Farbwechsel wieder rückgängig machen. | EffectClrAlmLevel |

| Steuerleistenfunktion | Funktion | Benutzerberechtigung an OS erforderlich |
|---|---|---|
| Effect rücks./ Effect überst. | Die Beschriftung dieser Schaltfläche ist entweder **Effect rücks.** oder **Effect überst.**, je nach dem Status des gewählten Effect. | |
| • Effect rücks. | Wird ein Effect durch einen Schnittpunkttyp S (Speichernd) oder R (Rücksetzbar und übersteuerbar) ausgelöst, so bleibt er auch aktiv, wenn er von dem Cause nicht mehr ausgelöst wird. Der Effect kann rückgesetzt werden (Reset), wenn er nicht mehr ausgelöst wird. Hierzu klicken Sie **Effect rücks.** an. Diese Funktion steht nur zur Verfügung, wenn für den ausgewählten Effect ein Rücksetzen möglich ist (in Grün angezeigt) und kein Rücksetzen/Übersteuern-TAG projektiert ist. | EffectResLevel |
| • Effect überst. | Wird ein Effect durch einen Schnittpunkttyp V (Übersteuerbar) oder R (Rücksetzbar und übersteuerbar) ausgelöst, so können die Output-TAGs des Effect auf die Betriebswerte gesetzt werden, obwohl der Effect noch ansteht. Dies wird als Übersteuern-Funktion bezeichnet. Ist für die ausgewählte Funktion diese Möglichkeit vorgesehen, so können Sie die Übersteuern-Funktion mit dieser Schaltfläche aktivieren, wenn kein Rücksetzen/Übersteuern-TAG projektiert ist. Mit Klick auf Schaltfläche **Effect überst.** wird der Effect deaktiviert.<br>**Hinweis**<br>Die Dauer der Übersteuern-Funktion sollte die unter den Optionen eingestellte maximale Zeit ("Maximale Zeit Übersteuern") nicht überschreiten. Wird die Zeit überschritten, wird ein Alarm ausgelöst.<br>Wird während der Übersteuern-Zeit ein anderer (mit dem Effect verschalteter) Cause aktiv, so endet die Übersteuern-Funktion sofort und es wird ebenfalls ein Alarm ausgelöst. | EffectOvrLevel |
| Treiber quitt. | Mit dieser Schaltfläche können Sie bei einem F-Anlauf nach der Fehlerbehebung die erforderliche Wiedereingliederung der F-Kanaltreiber vornehmen. | DriversAckLevel |
| Farben anzeigen | Mit dieser Schaltfläche können Sie im *Safety Matrix Viewer* die Zuordnung von Status bzw. Alarm-Profil zu Farbe in der Safety Matrix anzeigen. | - |

**⚠ WARNUNG**

**Wiedereingliederung der F-Kanaltreiber**

Ist im Sicherheitsprogramm für einen F-Anlauf nach einem STOP der F-CPU ein (Wieder-) Anlaufschutz programmiert, so wird die Ausgabe von Prozesswerten blockiert, bis eine manuelle Freigabe erfolgt. Die Freigabe darf erst erfolgen, wenn die Ausgabe der Prozesswerte gefahrlos möglich ist.

## Steuerleistenfunktion Bypass-Report

Die Steuerleistenfunktion Bypass-Report steht nur im Engineering Tool zur Verfügung. Die Funktion Bypass-Report legt eine Liste aller Causes und Effects an, für die Bypasses eingerichtet sind, und aller aktuell simulierten TAGs. Die Ergebnisse werden im Log-Fenster angezeigt.

## Siehe auch

Secure Write (Seite 136)

Initiator- und Confirmer-Berechtigung (Seite 134)

### 8.5.3.2 Beispiel: Effect rücksetzen

#### Bedienung mit zwei Bedienern

Für die Transaktion an der PCS 7 OS sind zwei Bediener mit unterschiedlichen Berechtigungen erforderlich. Die nachfolgenden Abschnitte beschreiben die erforderlichen Transaktionsschritte der beiden Bediener.

Die Bediener müssen zusätzlich zu der Initiator- und/oder Confirmer-Berechtigung die festgelegte Berechtigungsstufe für die jeweils auszuführende Bedienfunktion besitzen (hier: "EffectResLevel").

#### Initiator: Bedienung starten

1. Melden Sie sich an der OS als Benutzer mit der Initiator-Berechtigung und der festgelegten Berechtigungsstufe für "Effect rücksetzen" an.
2. Öffnen Sie das Bild, in dem das gewünschte Safety Matrix-Bausteinsymbol enthalten ist.
3. Klicken Sie auf das Safety Matrix-Bausteinsymbol, um den Bildbaustein zu öffnen.
4. Markieren Sie den Effect, den Sie rücksetzen möchten.
   Voraussetzung ist, dass der Effect in Grün angezeigt wird (= Rücksetzen möglich).
5. Klicken Sie auf die Schaltfläche **Effect rücks.** in der Steuerleiste.

   **Ergebnis**: Der *Safety Matrix Viewer* sendet das Kommando an die Safety Matrix und liest die Rücklesewerte. Die Timeout-Überwachung für die Transaktion wird gestartet.
6. Es erscheint der Bestätigungsdialog für die Transaktion. Überprüfen Sie, ob die angegebene Änderung mit der gewünschten Bedienung übereinstimmt.
   – Falls ja, aktivieren Sie das Kontrollkästchen "Die Bedienung wurde geprüft und soll aktiviert werden!", und betätigen Sie die Schaltfläche "Initiieren".
   – Falls nein, müssen Sie die Schaltfläche "Abbrechen" betätigen.

**Ergebnis**: Die Transaktion für den Initiator ist nun beendet, sie kann von einem Confirmer fortgesetzt werden.

---

**Hinweis**

Je nach auszuführender Bedienfunktion werden Sie evtl. aufgefordert, eine Begründung einzugeben, die mit dem Ereignis zusammen aufgezeichnet wird.

---

#### Confirmer: Bedienung bestätigen

1. Melden Sie sich an der OS als Benutzer mit der Confirmer-Berechtigung und der festgelegten Berechtigungsstufe für "Effect rücksetzen" an.
   Sie können an einer zweiten OS oder an der gleichen OS wie der Initiator angemeldet sein.
2. Öffnen Sie das Bild, in dem das gewünschte Safety Matrix-Bausteinsymbol enthalten ist.
3. Klicken Sie auf das Safety Matrix-Bausteinsymbol, um den Bildbaustein zu öffnen.
4. Klicken Sie auf die Schaltfläche "Confirm" unterhalb der Steuerleiste.
5. Es erscheint der Bestätigungsdialog für die Transaktion. Überprüfen Sie, ob die angegebene Änderung mit der gewünschten Bedienung übereinstimmt.
   – Falls ja, aktivieren Sie das Kontrollkästchen "Die Bedienung wurde geprüft und soll aktiviert werden!" und betätigen Sie anschließend die Schaltfläche "Confirm".
   – Falls nein, müssen Sie die Schaltfläche "Abbrechen" betätigen.

#### Ergebnis

Wenn die Transaktion innerhalb des festgelegten Zeitintervalls beendet ist, wird die erfolgreiche Bedienung innerhalb der Safety Matrix anhand der Statusanzeige (z. B. Farbwechsel) ersichtlich.

Die Bedienung durch den Confirmer wird darüber hinaus in die *PCS 7*-Bedienliste und in das Ereignisprotokoll der Safety Matrix eingetragen.

### 8.5.3.3 Wartungsänderungen

#### Einleitung

Im Online-Betrieb des *Safety Matrix Engineering Tools* bzw. von der PCS 7 OS über den *Safety Matrix Viewer* können Sie folgende Wartungsänderungen vornehmen:

| Online-Betrieb des *Safety Matrix Engineering Tools* | *Safety Matrix Viewer* |
|---|---|
| Wert eines Cause- oder Effect-TAG simulieren | Wert eines Cause- oder Effect-TAG simulieren |
| Werte für Limit, Hysterese und zulässige Diskrepanz (Delta) für analoge Input-Typen ändern | - |
| obere und untere Bereichsgrenze an F-Kanaltreibern für analoge Input-TAGs ändern* | - |

* Diese Bedienung erfolgt nicht mittels einer Secure-Write Transaktion.

### Wert eines Cause- oder Effect-TAG simulieren

Sie können den Wert eines Cause- oder Effect-TAG im Online-Betrieb des *Safety Matrix Engineering Tools* bzw. von der PCS 7 OS über den *Safety Matrix Viewer* simulieren.

---

**Hinweis**

Die Bediener an der PCS 7 OS müssen zusätzlich zu der Initiator- und/oder Confirmer-Berechtigung die festgelegte Berechtigungsstufe für die jeweils auszuführende Bedienfunktion besitzen (hier: "CauseTagSimLevel" bzw. "EffectTagSimLevel").

---

## Vorgehensweise

1. Doppelklicken Sie auf den gewünschten Cause/Effect, Spalte "Wert" oder klicken Sie bei markiertem Cause/Effect auf die Schaltfläche **TAGs anzeigen** in der Steuerleiste.
2. Aktivieren Sie im Dialog "Anzeige TAGs", Register "Werte" das Kontrollkästchen "Aktiviere Wartungsänderungen".
3. Klicken Sie auf die Schaltfläche (Simulation) **Start** für den betreffenden TAG.
   **Ergebnis**: Es wird eine Secure Write-Transaktion für das Starten der Simulation gestartet. Gemäß Ihrer Projektierung wird als Simulationswert entweder der aktuell anstehende Prozesswert oder der projektierte Simulationswert übernommen.
4. Wenn Sie den Wert des simulierten TAG ändern möchten, geben Sie den gewünschten Wert für den betreffenden TAG in das Feld "Simulationswert" ein (maximal 7 Zeichen, einschließlich Dezimaltrennzeichen und Vorzeichen).
   Achten Sie bei Analogwerten zusätzlich darauf, dass die angezeigten Bereichsgrenzen eingehalten werden. Wenn Sie den Simulationswert außerhalb der Bereichsgrenzen festlegen, erscheint ein Bestätigungsdialog, der Sie darauf aufmerksam macht. Sie können nun die Einstellung bestätigen oder den Dialog abbrechen und einen neuen Simulationswert eingeben.

---

**Hinweis**

In der Spalte "V_MOD" wird der von der F-Peripherie empfangene Analogeingabewert angezeigt (verfügbar ab *S7 F Systems Lib* V1_3). Wenn keine Kommunikation mit der F-Peripherie möglich ist oder nach einem Fehler noch keine Anwenderquittierung erfolgt ist, wird "0.0" angezeigt.

---

5. Klicken Sie auf die Schaltfläche **Schreiben** für den betreffenden TAG.
   **Ergebnis**: Es wird eine Secure Write-Transaktion für das Schreiben der Werte gestartet.
6. Zum Beenden der Simulation klicken Sie auf die Schaltfläche (Simulation) **Stop** für den betreffenden TAG.

---

**Hinweis**

Beim Simulieren eines TAG müssen Sie Folgendes beachten:

- Bei aktivierter Option "Gegenseitig verriegelte TAG-Simulation" kann jeweils nur ein TAG eines Cause bzw. Effect simuliert werden.
- Bei 'eigenen Kanaltreibern' betrifft die Simulation alle Benutzer des TAG. Dazu gehören andere Matrizen und jede benutzerprojektierte Logik, die diesen F-Kanaltreiber verwendet.
- Mit einem Präfix oder Suffix ("@", "#") versehene TAGs sind für diese Safety Matrix extern und werden nur intern in der Safety Matrix simuliert, d. h. die Simulation betrifft nur die Matrix-eigenen Funktionen. Außerhalb der Safety Matrix kann nur der physikalische (d. h. nicht simulierte) Wert verarbeitet werden.
- Damit die Safety Matrix auch externe F-Kanaltreiber (außer kundenspezifische Kanaltreiber mit Präfix "~") als 'eigene Kanaltreiber' verschaltet, müssen Sie beim Transfer der Safety Matrix in das Projekt die Option "Importierte Kanaltreiber verwenden (IEA Unterstützung)" aktivieren. Erst dadurch wirkt sich die Funktion "TAG simulieren" auch auf diese externen F-Kanaltreiber aus.

---

## Werte für Limit, Hysterese und zulässige Diskrepanz ändern

Sie können die Werte für Limit, Hysterese und zulässige Diskrepanz (Delta) für analoge Input-Typen auch im Online-Betrieb des *Safety Matrix Engineering Tools* anzeigen und bearbeiten.

## Vorgehensweise

1. Doppelklicken Sie auf den gewünschten Cause, Spalte "Limit".
2. Zur Aktualisierung der angezeigten Werte klicken Sie im Dialog "Anzeige Analog-Parameter - Cause x", Register "Werte" auf die Schaltfläche **Lesen**.
3. Aktivieren Sie das Kontrollkästchen "Aktiviere Wartungsänderungen".
4. Geben Sie den gewünschten Wert für Limit, Hysterese und (bei mehreren analogen Input-TAGs für einen Cause) die zulässige Diskrepanz in das jeweilige Feld "Neuer Wert" ein (maximal 7 Zeichen, einschließlich Dezimaltrennzeichen und Vorzeichen).
5. Klicken Sie auf die Schaltfläche **Schreiben**.
   **Ergebnis**: Es wird eine Secure Write-Transaktion für das Schreiben der Werte gestartet.

## Obere und untere Bereichsgrenze ändern

Sie können die aktuell im *CFC*-Plan gespeicherten oberen und unteren Bereichsgrenzen für analoge Input-TAGs auch im Online-Betrieb des *Safety Matrix Engineering Tools* anzeigen und bearbeiten.

## Vorgehensweise

1. Doppelklicken Sie auf den gewünschten Cause, Spalte "Wert" oder klicken Sie bei markiertem Cause auf die Schaltfläche **TAGs anzeigen** in der Steuerleiste.
2. Klicken Sie im Dialog "Anzeige TAGs", Register "Bereiche" auf die Schaltfläche **Bereich...** für den betreffenden Input-TAG.
3. Zur Aktualisierung der angezeigten Werte klicken Sie im Dialog "Ansicht TAG-Bereich" auf die Schaltfläche **Lesen**.
4. Aktivieren Sie im Dialog "Ansicht TAG-Bereich" das Kontrollkästchen "Aktiviere Wartungsänderungen".
5. Geben Sie den gewünschten Wert für die obere bzw. untere Bereichsgrenze in das jeweilige Feld "Neuer Wert" ein (maximal 7 Zeichen, einschließlich Dezimaltrennzeichen und Vorzeichen).
6. Klicken Sie auf die Schaltfläche **Schreiben** für die obere bzw. untere Bereichsgrenze.
   **Ergebnis**: Die Daten werden mittels *CFC*-Online-Änderung an die betreffenden F-Kanaltreiber geschrieben. Dazu werden Sie aufgefordert, den Sicherheitsbetrieb zu deaktivieren.

---

**Hinweis**

Beachten Sie, dass der Sicherheitsbetrieb erst wieder aktiviert wird, wenn Sie den Online-Betrieb der Safety Matrix ausschalten.

---

### Siehe auch

Secure Write (Seite 136)

## 8.6 Ereignisse und Meldungen

Im *PCS 7*-Meldesystem werden Alarme und die Bedienmeldungen, die von der OS ausgelöst wurden, protokolliert.

Das Ereignisprotokoll enthält die letzten 100 Meldungen der Safety Matrix.

### 8.6.1 Meldungen im Ereignisprotokoll der Safety Matrix

#### Einträge im Ereignisprotokoll

Die Safety Matrix führt ein Ereignisprotokoll (Event Log), in dem detailliert die einzelnen Ereignisse und Bedienungen protokolliert werden. Das Ereignisprotokoll kann als Text im *Safety Matrix Viewer* oder im *Safety Matrix Engineering Tool* ausgegeben werden.

Diesen Puffer kann sich auch der Bediener im *Safety Matrix Viewer* anzeigen lassen, und die letzten Ereignisse nachvollziehen. Das Ereignisprotokoll ist ein Umlaufpuffer mit max. 100 Einträgen, d. h. die ältesten Einträge werden überschrieben. Das Ereignisprotokoll kann nicht von der PCS 7 OS archiviert werden.

## 8.6.2 Bedienmeldungen des Safety Matrix Viewer

Wenn der *Safety Matrix Viewer* eine Bedienmeldung in der *PCS 7*-Bedienliste erzeugt, trägt er gleichzeitig ein Ereignis in das Ereignisprotokoll ein.

### Einträge in der *PCS 7*-Bedienliste

Der *Safety Matrix Viewer* trägt die Bedienungen in die *PCS 7*-Bedienliste ein. Alle Bedieneinträge enthalten folgende Informationen:

- Zeitpunkt der Bedienung
- Art der Bedienung
- Vom Bediener eingegebene Begründung der Bedienung ("Reason"), ausgegeben in der Spalte "Bedienung"
- angemeldeter Bediener
- Je nach Art der Bedienung werden zusätzliche Angaben gemacht, die in der Spalte "Bedienung" protokolliert werden:

| Safety Matrix-Steuerungsfunktionen | zusätzliche Einträge in Spalte "Bedienung" |
|---|---|
| Cause Bypass | Cause-Nummer; Cause-Beschreibung |
| FO-Alarm rücksetzen | Nummer der FO-Alarmgruppe |
| Effect übersteuern | Effect Nummer; Effect-Beschreibung |
| Effect rücksetzen | Effect Nummer; Effect-Beschreibung |
| Cause-TAG Simulation starten und beenden | Cause-Nummer; Cause-Beschreibung, TAG-Nummer; TAG-Name, gestartet oder beendet |
| Cause-TAG simulieren | Cause-Nummer; Cause-Beschreibung, TAG-Nummer; TAG-Name, vorheriger Wert, neuer Wert |
| Effect Bypass | Effect Nummer; Effect-Beschreibung |
| Effect-TAG Simulation starten und beenden | Effect-Nummer, Effect-Beschreibung, TAG-Nummer, TAG-Name, gestartet oder beendet |
| Effect-TAG simulieren | Effect-Nummer, Effect-Beschreibung, TAG-Nummer, TAG-Name, vorheriger Wert, neuer Wert |
| Treiber reintegrieren | - |
| Cause quittieren | Cause-Nummer; Cause-Beschreibung |

### Siehe auch

Meldungen im Ereignisprotokoll der Safety Matrix (Seite 148)

### 8.6.3 PCS 7-Alarmmeldungen im WinCC-Meldesystem

#### Signalisierung aller prozessrelevanten Ereignisse

Alle prozessrelevanten Ereignisse können per *WinCC*-Meldung signalisiert werden, so dass in einem Meldearchiv auch nach längerer Zeit nachvollzogen werden kann, welche Ereignisse in welcher Reihenfolge aufgetreten sind.

In *WinCC* erscheinen diese Meldungen wie jede andere im *PCS 7*-Meldesystem. Beim Betätigen der "Loop in Alarm"-Schaltfläche wird das Bild geöffnet, in dem das Bausteinsymbol der zur Meldung passenden Safety Matrix platziert ist. Klicken Sie dieses Symbol an, um die Bildbausteine des *Safety Matrix Viewer* zu öffnen.

#### Voraussetzung für das Erzeugen von Bausteinsymbolen

Voraussetzung für das Erzeugen der Bausteinsymbole für die Safety Matrix ist die entsprechende Projektierung der Meldebausteine und der Transfer der Safety Matrix mit aktivierter Option "Alarm-Bausteine platzieren":

- im Dialog "Eigenschaften" der Safety Matrix, Register "Alarme"
  (siehe Kapitel "Der Dialog "Eigenschaften" der Safety Matrix (Seite 75)")
- im Dialog "Cause-Details", Register "Alarme"
  (siehe Kapitel "Dialog "Cause-Details" - Register "Alarme" (Seite 93)")
- im Dialog "Effect-Details ", Register "Alarme"
  (siehe Kapitel Dialog "Effect-Details" - Register "Alarme" (Seite 101)")
- im Dialog "Transferieren ins Projekt", Register "Optionen"
  (siehe Kapitel "Transferieren der Safety Matrix in das Projekt (Seite 111)")

Beim OS Übersetzen der Safety Matrix werden für die projektierten Meldebausteine F_MA_AL (Safety Matrix, 1-mal), F_SC_AL (Causes, x-mal) und F_SE_AL (Effects, x-mal) die entsprechenden Bausteinsymbole erzeugt. Diese bieten unterschiedliche Sichten, nämlich:

- auf die gesamte Safety Matrix
- auf einen einzelnen Cause mit zugehörigen Schnittpunkten und Effects
- auf einen einzelnen Effect mit zugehörigen Schnittpunkten und Causes.

#### Siehe auch

Kapitel "Der Dialog "Eigenschaften" der Safety Matrix (Seite 75)"

### 8.6.4 Warnmeldungen

#### Warnmeldungen der Safety Matrix

Die Safety Matrix gibt im Online-Betrieb Warnmeldungen als roten Text unterhalb der Steuerleiste aus, z. B.:

- Transaktion läuft
- Matrix wird nicht bearbeitet
- Kommunikationsfehler

# 9 Dokumentation einer Safety Matrix

## 9.1 Safety Matrizen vergleichen

### Einleitung

Mithilfe des Menübefehls "Vergleiche Matrix mit" können Sie folgende Safety Matrizen auf Basis von Informationen, die in .cem-Dateien hinterlegt sind, miteinander vergleichen und Abweichungen anzeigen und ausdrucken:

- die aktuelle Safety Matrix mit einer anderen, aktuell geöffneten Safety Matrix
- die aktuelle Safety Matrix mit der zuletzt gespeicherten Version der Safety Matrix
- die aktuelle Safety Matrix mit der zuletzt in das Projekt transferierten Safety Matrix
- die aktuelle Safety Matrix mit der in die F-CPU geladenen Safety Matrix

### Vorgehensweise

Rufen Sie den Menübefehl **Extras > Vergleiche Matrix mit** auf und wählen Sie den gewünschten Vergleich aus:

- **Matrix**

  Hierzu müssen Sie beide zu vergleichenden Safety Matrizen im *Safety Matrix Engineering Tool* geöffnet haben.
- **Speicherung**

  Hier wird die Safety Matrix mit ihrer gespeicherten Version verglichen. Der Vergleich zeigt Ihnen also die Änderungen an, die Sie nach dem letzten Speichern vorgenommen haben.
- **Programm**
- **CPU**

Das Ergebnis des Vergleichs zeigt ihnen die Gleichheit/Unterschied von:

- Safety Matrix-Signatur
- Parameterwerten
- Causes, Effects und Schnittpunkten

## 9.2 CFC-Pläne vergleichen

### Einleitung

Mithilfe des Dialogs "Vergleiche Programme" können Sie alle *CFC*-Pläne eines Planordners, die vom *Safety Matrix Engineering Tool* beim Transfer erzeugt werden, miteinander vergleichen und Abweichungen anzeigen und ausdrucken. Dieser Vergleich unterstützt Sie bei Inbetriebnahme und Abnahme einer Anlage.

Das Ergebnis des Vergleichs zeigt Ihnen die Gleichheit/Unterschied von:

- Gesamtsignatur
- Safety Matrix-Signaturen
- Parameterwerten
- Causes, Effects und Schnittpunkten
- TAG-Namen und TAG-Eigenschaften

Mit dem Dialog "Vergleiche Programme" können Sie auch herausfinden, ob ein Sicherheitsprogramm *nicht* geändert wurde. Vergleichen Sie dazu das Sicherheitsprogramm mit dem ursprünglichen Programmstand, den Sie z. B. als Referenz abgespeichert haben.

### Starten des Vergleichs

Rufen Sie den Menübefehl **Extras > Vergleiche Programme** auf. Der Dialog "Vergleiche Programme" wird geöffnet.

#### Schaltfläche "Referenz speichern"

Mithilfe dieser Schaltfläche können Sie das aktuelle Programm (d. h. alle Safety Matrix-Pläne im S7-Programm) als Referenz speichern. Diese Referenz stellt eine Untermenge des Referenzprogramms dar, das im Dialog "Sicherheitsprogramm" von *S7 F Systems* mit der Schaltfläche "Referenz speichern" erstellt wird.

Die Referenz für den Dialog "Sicherheitsprogramm" in *S7 F Systems* wird in einer eigenen Datei unabhängig von *S7 F Systems* gespeichert.

#### Programm/Referenz

Wählen Sie eines dieser Optionsfelder aus, um festzulegen, ob Sie das aktuelle oder das Referenzprogramm vergleichen möchten.

#### Vergleichen mit:

Mit dieser Auswahlliste können Sie das zweite Sicherheitsprogramm bestimmen, mit dem Sie das soeben gewählte Sicherheitsprogramm vergleichen möchten.

| Programm | vergleichen mit ... | |
|---|---|---|
| | Referenz | Das aktuelle Programm wird mit der zuletzt gespeicherten Referenz verglichen. |
| | anderes Projekt | Das aktuelle Programm wird mit einem anderen Programm verglichen. Wählen Sie das Offline-Programm mit der Schaltfläche "Durchsuchen". |
| **Referenz** | **vergleichen mit ...** | |
| | aktuellem Sicherheitsprogramm | Die zuletzt gespeicherte Referenz wird mit dem aktuellen Sicherheitsprogramm verglichen ("Rückwärtsvergleich"). |
| | anderes Projekt | Die zuletzt gespeicherte Referenz wird mit einem anderen Programm verglichen. Wählen Sie das Offline-Programm mit der Schaltfläche "Durchsuchen". |

#### Schaltfläche "Durchsuchen"

Mithilfe dieser Schaltfläche und des Dialogs "Öffnen" können Sie das zu vergleichende Offline-Programm eines beliebigen Projekts auswählen, sofern Sie unter "Vergleichen mit" die Option "anderes Projekt" ausgewählt haben.

#### Schaltfläche "Start"

Klicken Sie diese Schaltfläche an, um den Vergleich zu beginnen.

### Ergebnis

Das Ergebnis des Vergleichs zeigt Ihnen, ob ein Cause/Effect neu, geändert oder gelöscht worden ist.

- Für Elemente aus der Quelle, zu denen kein Element in der Referenz gefunden wird, wird ‚Cause/Effect x neu' (x bezieht sich auf die Quelle) ausgegeben.
- Für Elemente aus der Referenz, zu denen kein Element in der Quelle gefunden wird, wird ‚Cause/Effect x gelöscht' (x bezieht sich auf die Quelle) ausgegeben.
- Für Elemente, bei denen ein Unterschied gefunden wird, wird ‚Cause/Effect x geändert' (x bezieht sich auf die Quelle und wird aus der Nummer vom Vorgängerelement bestimmt.) ausgegeben.

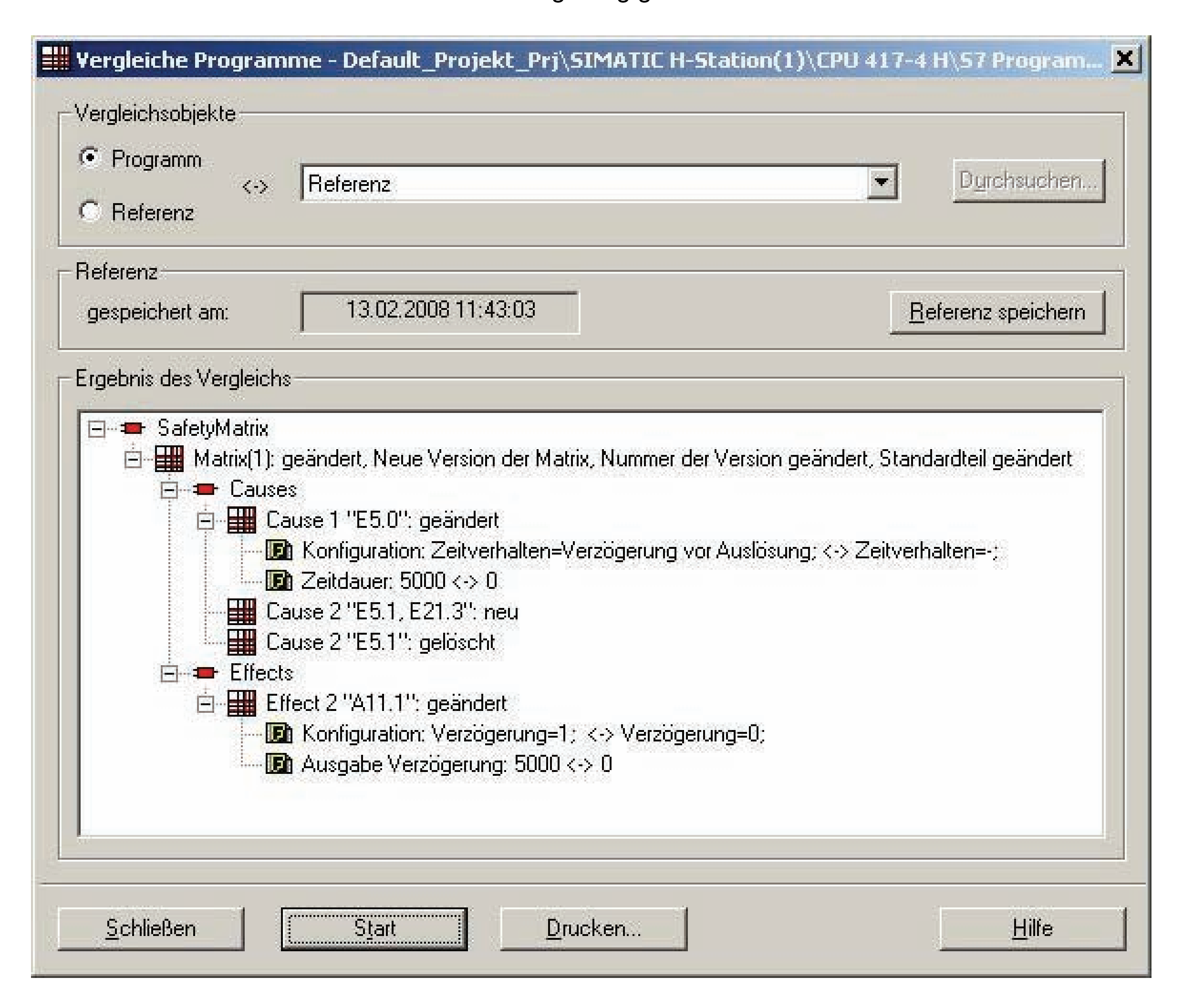
Abschließend werden die Schnittpunkte aufgrund der zugeordneten Paare Cause/Effect verglichen.

- Wenn zu einem Cause/Effect-Paar ein Schnittpunkt in der Referenz gefunden wird, dann wird diese mit dem entsprechenden Schnittpunkt der Quelle verglichen. Wenn dabei ein Unterschied festgestellt wird, dann wird ‚Schnittpunkt von Cause x und Effect y geändert' (x und y beziehen sich auf die Quelle) ausgegeben.
- Wenn zu diesem Paar kein Schnittpunkt gefunden wird, dann wird ‚Schnittpunkt von Cause x und Effect y neu' (x und y beziehen sich auf die Quelle) ausgegeben.
- Es werden alle gelöschten Schnittpunkte angegeben, deren Cause und Effect nicht gelöscht wurden.

Die Unterschiede zwischen den Safety Matrix-Plänen werden Ihnen hierarchisch angezeigt, ähnlich wie im Explorer.

Das folgende Bild zeigt einen Beispielvergleich. Dabei wurden folgende Änderungen in der Safety Matrix vorgenommen:

- im Cause 1 ist das Zeitverhalten geändert worden
- im Cause 2 ist der TAG 2 neu belegt worden
- im Effect 2 ist die Verzögerung geändert worden.



## 9.3 Konfigurationsreport

### Gesamtdarstellung der kompletten Konfiguration

Der Konfigurationsreport enthält die komplette Konfiguration der Safety Matrix.

### Erstellen eines Konfigurationsreports

Wählen Sie den Menübefehl **Extras > Reporte > Konfigurationsreport**.

Der Konfigurationsreport wird im Log-Fenster geöffnet.

### Detaillierte Angaben

Der Konfigurationsreport enthält folgende Angaben:

- Pfad zum S7-Programm, zu dem die Safety Matrix gehört, in der Komponentensicht
- Detaillierte Angaben zu allen Causes
- Detaillierte Angaben zu allen Effects
- Detaillierte Angaben zu allen Schnittpunkten
- Auflistung der Kommentare
- Auflistung der Versionen
- Auflistung der Sicherheitstechnischen Funktionsgruppen (SIF)
- Auflistung der wesentlichen Eigenschaften der Safety Matrix, u. a.:
  - Größe (Anzahl der Zeilen und Spalten) der Safety Matrix
  - Nutzungsstatistik zu Causes, Effects, Schnittpunkten (Anzahl der projektierten Causes, Effects, Schnittpunkte)
  - Pfade (zu Safety Matrix-Datei, SIMATIC-Projekt, S7-Programm)
  - Haupt- und Nebenversionen
  - Dateiversion
  - Zykluszeit
  - Task-OB
  - Safety Matrix-Signatur

### Ausdruck des Konfigurationsreports

Drucken Sie den Konfigurationsreport nach Fertigstellung der Safety Matrix aus und heben Sie ihn sorgfältig auf. Er ist Bestandteil der Dokumentation für die Abnahme des Sicherheitsprogramms und der Anlage.

# 9.4 Validierungsreport

## Plausibilitätsprüfung der kompletten Konfiguration

Der Validierungsreport zeigt das Ergebnis einer Plausibilitätsprüfung der Safety Matrix-Konfiguration in Form von Fehlern und Warnungen an.

## Erstellen eines Validierungsreports

Wählen Sie den Menübefehl **Extras > Reporte > Validierungsreport**.

Der Validierungsreport wird im Log-Fenster geöffnet.

## Fehler- und Warnmeldungen

Der Validierungsreport enthält Fehler und Warnungen, wie z. B.:

- fehlende Schnittpunkt-Konfigurationen
- Effects ohne Rücksetzen-TAGs
- mehrere Effects mit dem gleichen Output-TAG

## Ausdruck des Validierungsreports

Sie können den Validierungsreport über den Menübefehl **Datei > Speichern als** bzw. **Drucken** speichern und ausdrucken.

# Abnahme einer Safety Matrix 10

## Einleitung

Bei der Abnahme der Anlage müssen Sie alle relevanten anwendungsspezifischen Normen und das nachfolgende Verfahren einhalten. Dies gilt auch für nicht abnahmepflichtige Anlagen. Bei der Abnahme müssen Sie die Auflagen in dem Bericht zum Zertifikat beachten.

Die Abnahme eines F-Systems wird in der Regel von einem unabhängigen Sachverständigen durchgeführt.

## Abnahme wie bei S7 F/FH Systems

Die Abnahme einer Safety Matrix verläuft grundsätzlich wie bei S7 F/FH Systems. Daher müssen Sie das Kapitel 10 des Programmier- und Bedienhandbuchs "S7 F/FH Systems, Projektieren und Programmieren (http://support.automation.siemens.com/WW/view/de/2201072)" beachten und befolgen (bzw. für ältere Versionen von *S7 F Systems* das entsprechende Kapitel im zugehörigen Handbuch). Die dort beschriebenen Vorgehensweisen sind für die Safety Matrix als Untermenge von *S7 F Systems* ebenso gültig. Dort finden Sie auch weitere Details zu den einzelnen Schritten der Abnahme.

Im Folgenden werden nur diejenigen Aktionen ausführlicher beschrieben, die **zusätzlich** für die Safety Matrix durchzuführen sind.

## Erstabnahme eines Sicherheitsprogramms

Die folgende Auflistung gibt die Schritte der *S7 F Systems*-Abnahme wieder. Hier sind nur die Safety Matrix-spezifischen Ergänzungen aufgeführt.

1. Prüfung der Projektierung der F-CPU und F-Peripherien vorab (optional)
2. Sicherung des *STEP 7* -Projekts
   – **Vor** der Sicherung Ihres *STEP 7* -Projekts müssen Sie alle Matrizen **transferieren** und **übersetzen** (siehe Kapitel "Safety Matrix transferieren (Seite 111) " und "Übersetzen und Laden (Seite 121) ").
   – Überprüfen Sie das Ergebnis des Transfers mithilfe des Menübefehls **Extras > Vergleiche Matrix mit > Programm.** Es dürfen keine Unterschiede angezeigt werden.
3. Kontrolle des Ausdrucks
   – **Drucken** Sie für jede Matrix den Konfigurationsreport aus und **kontrollieren** Sie ihn (siehe Kapitel "Konfigurationsreport (Seite 157) "). Überprüfen Sie, dass darin

     - alle Angaben vollständig sind und der gewünschten Projektierung entsprechen. Achten Sie dabei z. B. auch auf die Projektierung von Zeiten und unbeabsichtigte Verschaltungen.

     - kein Schnittpunkt (Cause/Effect-Paar) mehrfach vorhanden ist
   – Die Signaturen und Anfangswertsignaturen der Safety Matrix F-Bausteine müssen mit denen im Annex 3 des Berichts zum Zertifikat übereinstimmen. Beim Einsatz der F-Bibliothek *Failsafe Blocks* (V1_2) ist die Signatur und Anfangswertsignatur des F-Bausteins F_TEST gemäß Annex 3 und nicht gemäß Annex 1 zu prüfen.
4. Laden des S7-Programms in die F-CPU
5. Durchführung eines vollständigen Funktionstests

## Abnahme von Änderungen am Sicherheitsprogramm

Die folgende Auflistung gibt die Schritte der *S7 F Systems*-Abnahme wieder. Hier sind nur die Safety Matrix-spezifischen Ergänzungen aufgeführt.

1. Sichern Sie Ihr Sicherheitsprogramm.

- **Vor** der Sicherung Ihres Sicherheitsprogramms müssen Sie alle Matrizen **transferieren** und **übersetzen** (siehe Kapitel "Safety Matrix transferieren (Seite 111) " und "Übersetzen und Laden (Seite 121) ")
- Überprüfen Sie das Ergebnis des Transfers mithilfe des Menübefehls **Extras > Vergleiche Matrix mit > Programm**. Es dürfen keine Unterschiede angezeigt werden.

2. Vergleichen Sie Ihr neues Sicherheitsprogramm mit Ihrem abgenommenen Sicherheitsprogramm.
   - **Identifizieren** Sie die Matrizen, die geändert wurden, mit Hilfe des Dialogs "Programme vergleichen" (Dialog "Sicherheitsprogramm" in *S7 F Systems*).
     Als Ergebnis des Vergleichs wird Ihnen eine Liste von geänderten F-Ablaufgruppen mit ihren F-Bausteinen angezeigt. Alle F-Bausteine von Safety Matrizen sind in der Voreinstellung pro OB in einer gemeinsamen F-Ablaufgruppe enthalten. Geänderte F-Bausteine enthalten den Namen der geänderten Safety Matrix.
   - **Identifizieren** Sie die Änderungen in der TAG-Vorverarbeitung: Die Vorverarbeitung eines TAG liegt im Plan "Matrixname\PP_Chart\PP_<TAG-Name>".
   - **Vergleichen** Sie die geänderten Safety Matrizen nacheinander wie folgt:

     - Vergleich im Dialog "Vergleiche Programme" der Safety Matrix (siehe Kapitel "CFC-Pläne vergleichen (Seite 154) ")

     - Vergleich mittels Menübefehl **Vergleiche Matrix mit > Safety Matrix** (siehe Kapitel "Safety Matrizen vergleichen (Seite 153) ")
3. Kontrollieren Sie die Änderungen im Ausdruck.
   - **Drucken** Sie für jede Matrix den Konfigurationsreport aus und **kontrollieren** Sie ihn (siehe Kapitel "Konfigurationsreport (Seite 157) "). Überprüfen Sie, dass darin alle Angaben vollständig sind und der gewünschten Projektierung entsprechen. Achten Sie dabei z. B. auch auf die Projektierung von Zeiten und unbeabsichtigte Verschaltungen.
4. Laden Sie Ihr geändertes Sicherheitsprogramm in die F-CPU.
5. Führen Sie einen Funktionstest Ihrer Änderungen durch.
   - Wenn die beiden unter Punkt 2. durchgeführten Vergleiche übereinstimmend diejenigen Änderungen auflisten, die Sie in der Safety Matrix vorgenommen haben, müssen sie nur diese Änderungen prüfen.
   - Listen die beiden Vergleiche darüber hinausgehende bzw. abweichende Änderungen auf oder wird "Matrix geändert" angezeigt, so müssen Sie jeweils die gesamte Safety Matrix prüfen.

# 11 Beispielparametrierungen

Im folgenden Kapitel finden Sie Zeitdiagramme, die Ihnen beispielhaft das Verhalten von Causes und Effects für unterschiedliche Projektierungen zeigen.

Bitte beachten Sie, dass in den folgenden Beispielen jeweils ein diskreter TAG mit Deenergize-to-trip (DTT) gewählt wurde.

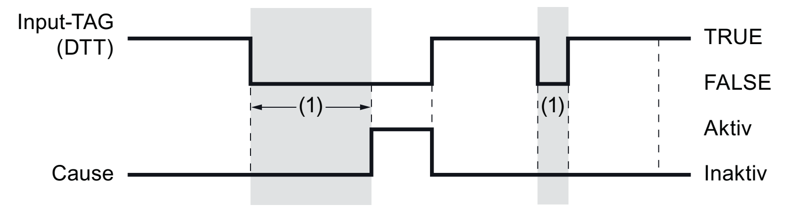
## 11.1 Beispielparametrierungen für Causes

### 11.1.1 Zeitverhalten

#### Zeitverhalten eines Cause

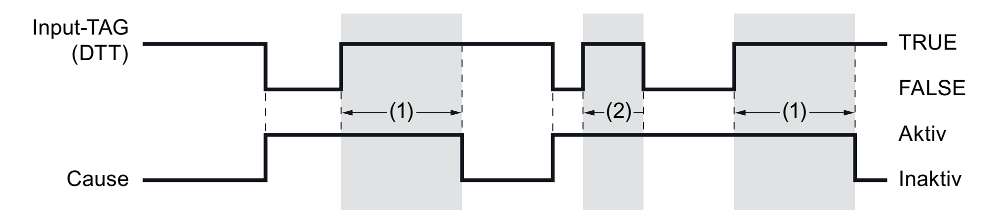
Pro Cause kann immer nur eine Einstellung gesetzt werden, die das Zeitverhalten betrifft.

#### Einschaltverzögerung



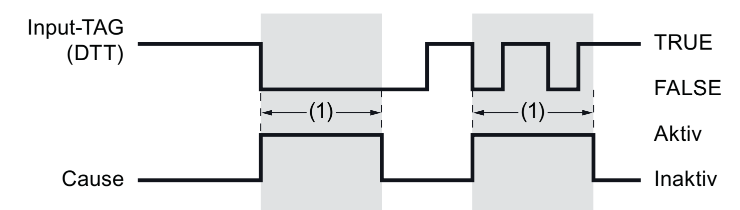

- Graustufe: Zeit läuft
- (1): Einschaltverzögerung
- Verzögertes Aktivieren des Cause
- Der Input-TAG muss die Einschaltverzögerungszeit über anstehen, damit der Cause aktiv wird.

## Ausschaltverzögerung




- Graustufe: Zeit läuft
- (1): Ausschaltverzögerung
- (2): Ausschaltverzögerung abgebrochen durch Änderung des Input-TAG.
- Der Cause ist noch über die projektierte Zeit der Ausschaltverzögerung aktiv, nachdem der Input-TAG TRUE geworden ist. Eine gegebenenfalls projektierte Quittierung des Cause hat keine Auswirkung auf dieses Verhalten.
- Der Timer der Ausschaltverzögerung wird abgebrochen, wenn der Input-TAG wieder FALSE geworden ist.

## Zeitgesteuerter Cause

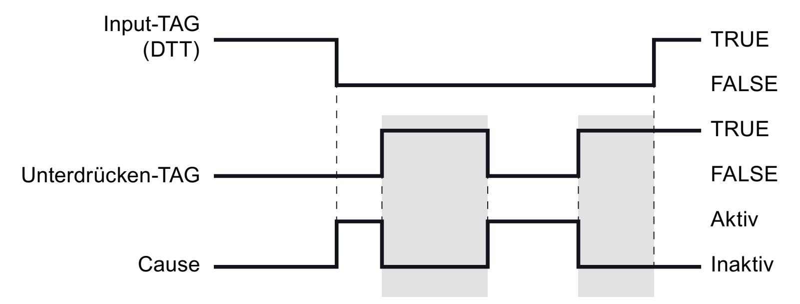



- Graustufe: Zeit läuft
- (1): Zeit für zeitgesteuerten Cause
- Wird der Input-TAG FALSE, so wird der Timer des zeitgesteuerten Cause gestartet und nach dem Ablauf des Timers wird der Cause wieder inaktiv, unabhängig davon, welchen Zustand der Input-TAG währenddessen annimmt. Eine gegebenenfalls projektierte Quittierung des Cause hat keine Auswirkung auf dieses Verhalten.

## 11.1.2 Unterdrückung (Inhibit)

### Verhalten beim Unterdrücken eines Cause

Der Unterdrücken-TAG wird verwendet, um den Cause während des Anfahrens in einem Batch-Prozess zu unterdrücken. Der Cause wird unterdrückt, d. h. inaktiv, wenn der Unterdrücken-TAG TRUE ist.

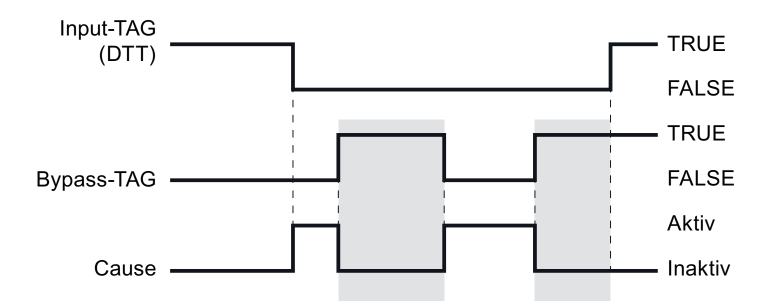



- Graustufe: Unterdrücken des Cause aktiv
- Einschaltverzögerung, Ausschaltverzögerung und zeitgesteuerter Cause haben keine Auswirkung auf die Funktion des Unterdrücken-TAG. Sie wirken unabhängig voneinander.
- Ist "Automatisch quittierter aktiver Cause" nicht gesetzt, ist für das Deaktivieren des Cause ein manuelles Quittieren nötig. Der Unterdrücken-TAG unterdrückt lediglich einen aktivierten Cause, ohne ihn zu quittieren.

### 11.1.3 Bypass

#### Verhalten bei Bypass

Bypass und Unterdrückung haben grundsätzlich die gleiche Funktionalität. Die Unterschied betrifft ausschließlich die Verwendung. Der Bypass findet seinen Einsatz zu Wartungszwecken. Der Cause wird inaktiv, wenn der Wert des Bypass-TAG = TRUE ist.




- Graustufe : Bypass für Cause aktiv
- Einschaltverzögerung, Ausschaltverzögerung und zeitgesteuerter Cause haben keine Auswirkung auf die Funktion des Bypass-TAG. Sie wirken unabhängig voneinander.
- Ist "Automatisch quittierter aktiver Cause" nicht gesetzt, ist für das Deaktivieren des Cause ein manuelles Quittieren nötig. Der Bypass-TAG unterdrückt lediglich einen aktivierten Cause, ohne ihn zu quittieren.
- Neben dem Bypass-TAG kann auch der Soft-Bypass über die Projektierung erlaubt werden. Dann kann der Benutzer den Bypass durch eine Bedienung steuern.

### 11.1.4 Automatisch quittierter aktiver Cause

#### Verhalten bei automatisch quittiertem aktivem Cause

Ist "Automatisch quittierter aktiver Cause" projektiert, so wird der Cause automatisch inaktiv, sobald die Auslösebedingungen nicht mehr erfüllt sind. Ist "Automatisch quittierter aktiver Cause" nicht projektiert, so muss der Bediener das Quittieren eines aktiven Cause manuell veranlassen. Der Cause bleibt solange aktiv, bis quittiert wurde.

Bei projektierter Ausschaltverzögerung bzw. zeitgesteuertem Cause hat die Projektierung für das Quittieren des aktivierten Cause keine Auswirkung.

### 11.1.5 Auslösen bei Bad Quality

#### Verhalten bei Bad Quality

Ist "Auslösen bei Bad Quality" aktiviert, so bewirken die vom F-Kanaltreiber gemeldeten Qualitätsfehler, dass der Input-TAG die Auslösebedingung erfüllt und der Cause je nach Funktionstyp aktiv werden kann.

### 11.1.6 Alarm bei Auslösung eines Inputs

#### Alarmverhalten bei mehreren Input-TAGs

Ist ein Cause mit mehreren Input-TAGs projektiert, so können Sie wählen, ob ein Alarm angezeigt wird, sobald einer der Eingänge die Auslösekriterien erfüllt. Standardmäßig ist der Alarm bei diskreten Eingängen ausgeschaltet, bei analogen Eingängen eingeschaltet.

## 11.2 Beispielparametrierungen für Effects

### 11.2.1 Rücksetzen/Übersteuern

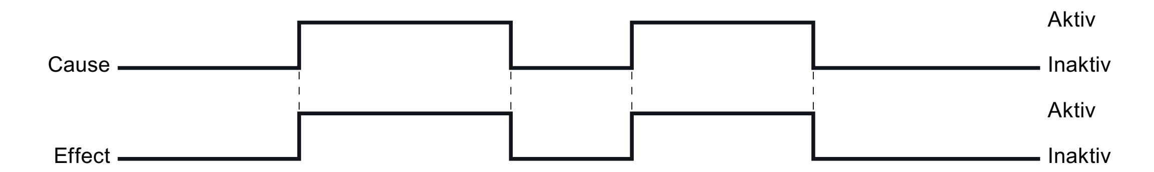
#### Verhalten beim Rücksetzen/Übersteuern eines Effect in Abhängigkeit zur Projektierung des Schnittpunkts

Rücksetzen/Übersteuern erfolgt entweder über eine Bedienung über die Schaltfläche im Online-Betrieb des *Safety Matrix Engineering Tools* oder im *Safety Matrix Viewer*, oder durch das Setzen und Rücksetzen des Rücksetzen/Übersteuern-TAG.

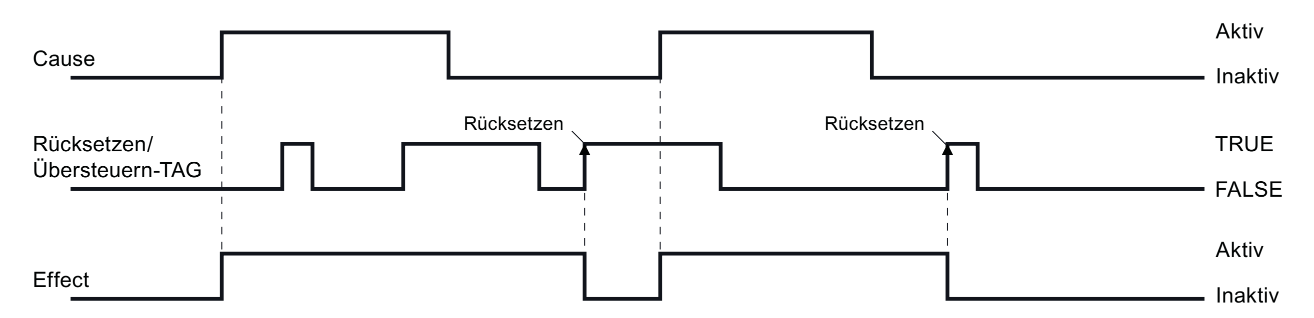
Rücksetzen/Übersteuern-TAG und maximale Übersteuerungszeit haben keine Auswirkungen auf den Effect.

### Rücksetzen/Übersteuern eines Effect bei Schnittpunkt "N - Nicht speichernd"

Rücksetzen/Übersteuern ist nicht relevant für Effects bei Schnittpunkt "N - Nicht speichernd".

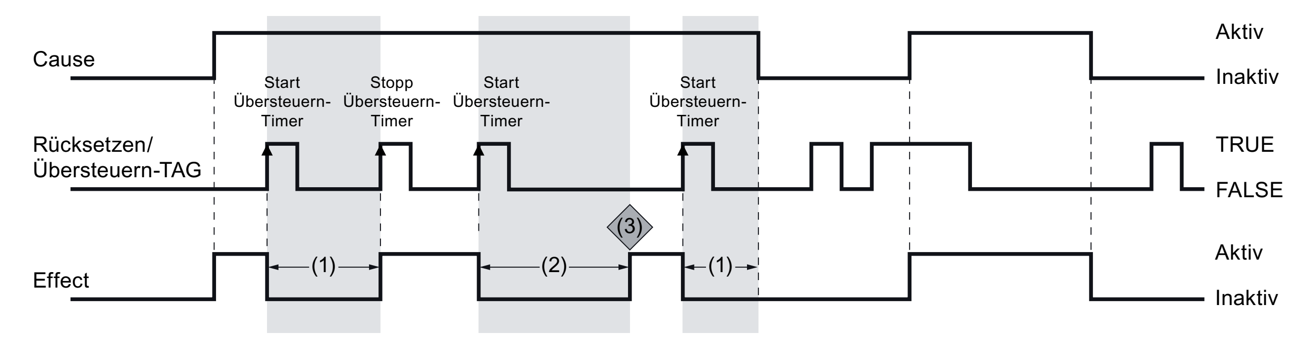



### Rücksetzen/Übersteuern eines Effect bei Schnittpunkt "S - Speichernd"



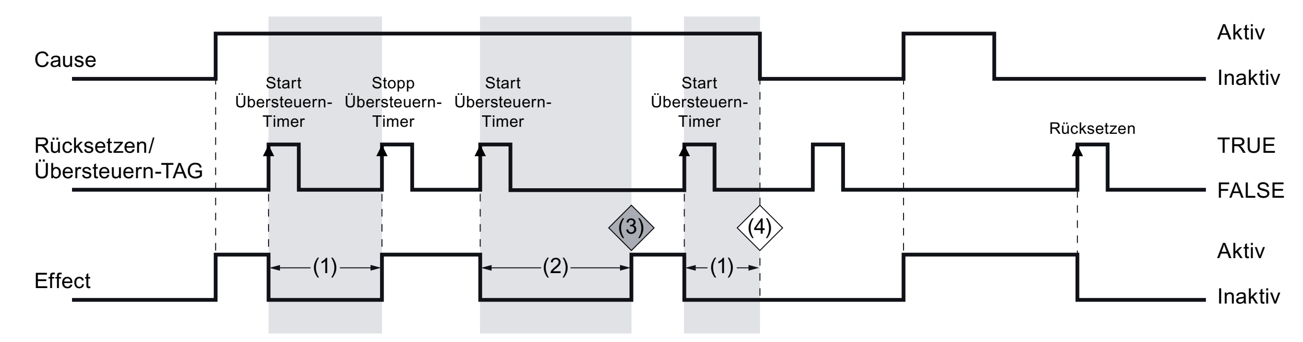

- Rücksetzen hat erst eine Auswirkung, wenn der Cause inaktiv geworden ist.
- Nachdem der Cause inaktiv wurde, ist ein Rücksetzen nötig, um auch den Effect zu deaktivieren.
- Für das Rücksetzen wird eine steigende Flanke benötigt.

### Rücksetzen/Übersteuern eines Effect bei Schnittpunkt "V - Übersteuerbar"




- Graustufe : Übersteuern-Timer läuft
- (1): Zeit < Maximale Übersteuerungszeit
- (2): Zeit >= Maximale Übersteuerungszeit
- (3): **Alarm**: Zeitüberschreitung beim Übersteuern des Effect; der Alarm wird entweder über eine Bedienung oder durch das nächste Starten des Übersteuern-Timers gelöscht.
- Jeweils eine steigende Flanke des Übersteuern-TAG startet und stoppt den Übersteuern-Timer.
- Der Timer wird automatisch gestoppt, sobald die maximale Übersteuerungszeit erreicht wurde.
- Wird der Cause inaktiv, so wird auch der Übersteuern-Timer beendet.

### Rücksetzen/Übersteuern eines Effect bei Schnittpunkt "R - Rücksetzbar und Übersteuerbar"




- Graustufe : Übersteuern-Timer läuft
- (1): Zeit < Maximale Übersteuerungszeit
- (2): Zeit >= Maximale Übersteuerungszeit
- (3): **Alarm**: Zeitüberschreitung beim Übersteuern des Effect; der Alarm wird entweder über eine Bedienung oder durch das nächste Starten des Übersteuern-Timers gelöscht.
- Dieser Schnittpunkt bildet die Kombination aus den Schnittpunkten S und V mit der Besonderheit, dass kein Rücksetzen nötig ist, wenn der Übersteuern-Timer beim Inaktivwerden des Cause noch läuft (4).

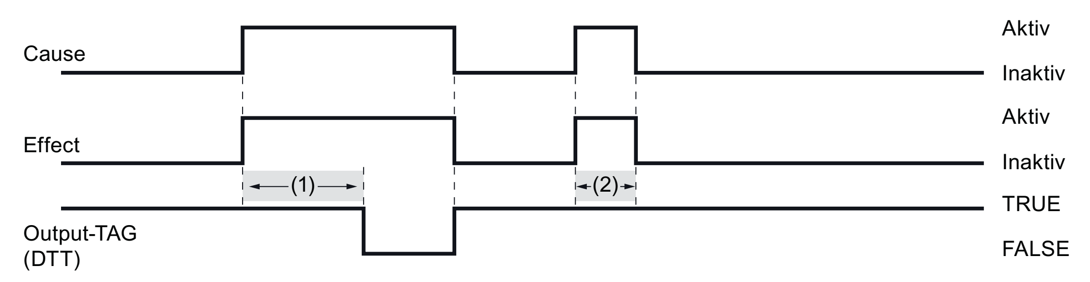
## 11.2.2 Rücksetzen/Übersteuern mit Ausgabeverzögerung

### Verhalten beim Rücksetzen/Übersteuern mit Ausgabeverzögerung in Abhängigkeit zur Projektierung des Schnittpunkts

Die Ausgabeverzögerung verzögert nach dem Aktivwerden des Effect die Änderung der Output-TAGs.

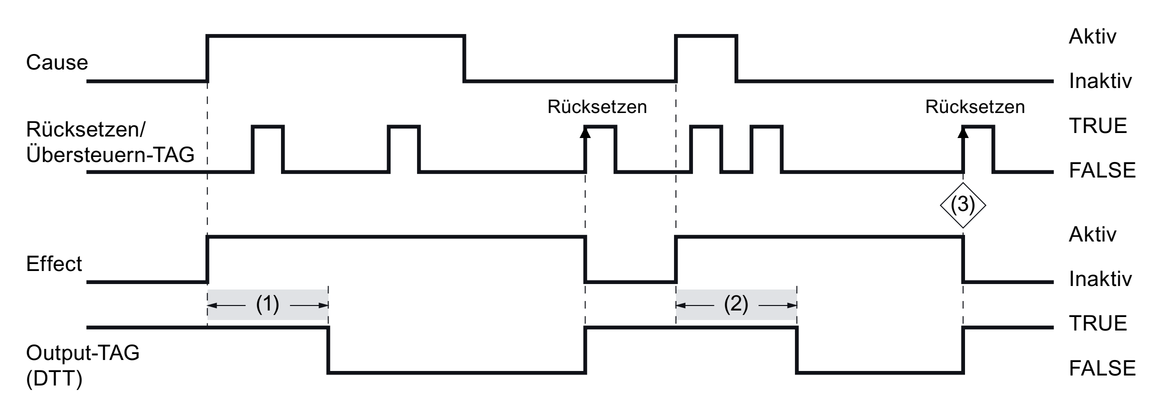
### Rücksetzen/Übersteuern eines Effect mit Ausgabeverzögerung bei Schnittpunkt "N - Nicht speichernd"

Rücksetzen/Übersteuern-TAG und maximale Übersteuerungszeit haben keine Auswirkung auf den Effect bei Schnittpunkt "N - Nicht speichernd".



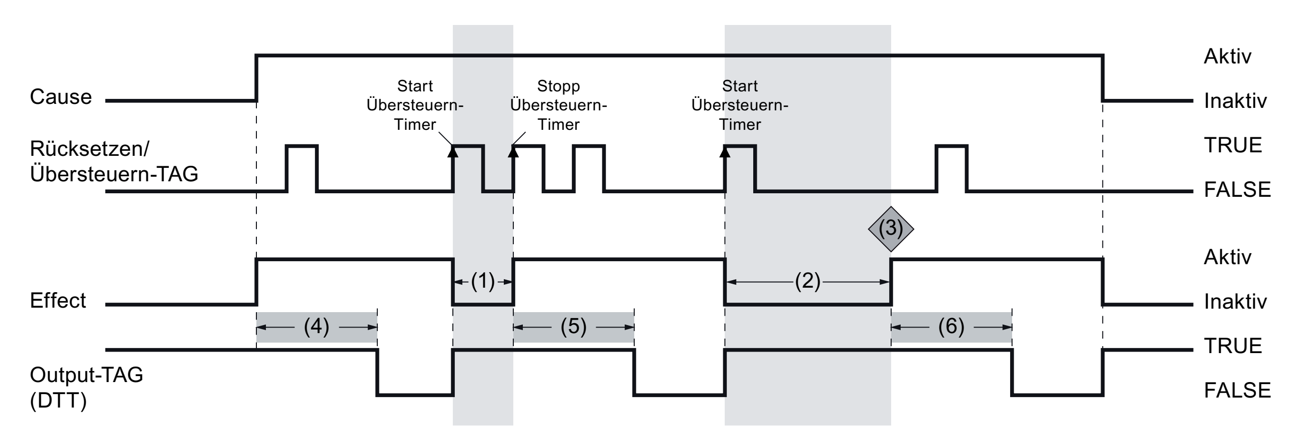

- (1): Zeit >= projektierte Zeitdauer für Ausgabeverzögerung
- Graustufe : Ausgabeverzögerung-Timer läuft
- (2): Wird der Cause inaktiv, so wird auch der Ausgabeverzögerung-Timer gestoppt.

### Rücksetzen/Übersteuern eines Effect mit Ausgabeverzögerung bei Schnittpunkt "S - Speichernd"



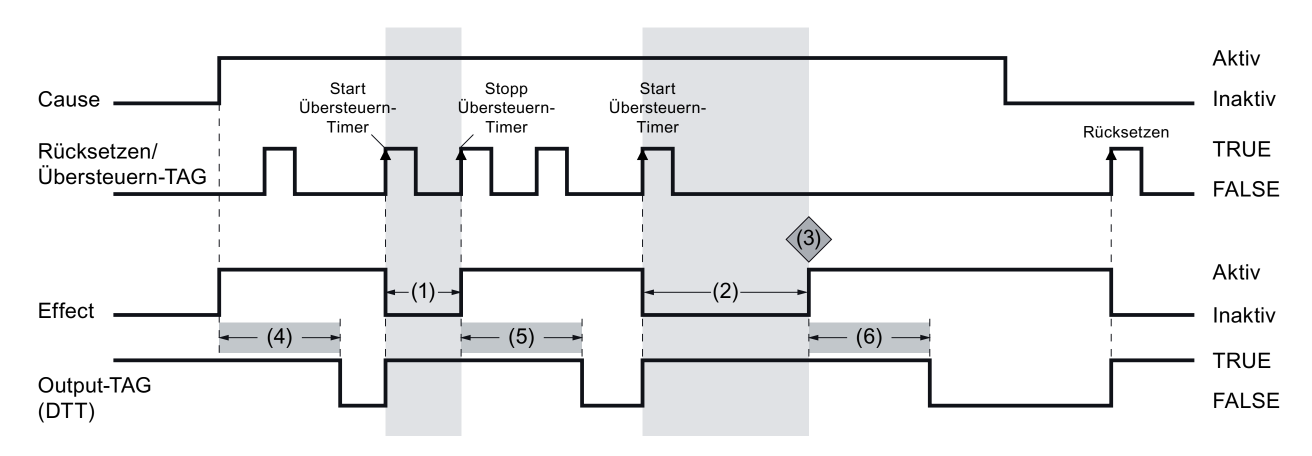

- (1): Zeit >= projektierte Zeitdauer für Ausgabeverzögerung
- Graustufe : Ausgabeverzögerung-Timer läuft
- Nachdem der Cause inaktiv wurde, ist ein Rücksetzen nötig, um auch den Effect zu deaktivieren.
- Für das Rücksetzen wird eine steigende Flanke benötigt.
- Rücksetzen hat keine Wirkung, solange der Cause aktiv ist oder der Ausgabeverzögerung-Timer läuft.
- (2): Wird der Cause inaktiv, so wird der Ausgabeverzögerung-Timer nicht gestoppt. Erst nachdem der Ausgabeverzögerung-Timer abgelaufen ist, kann zurückgesetzt werden (3).

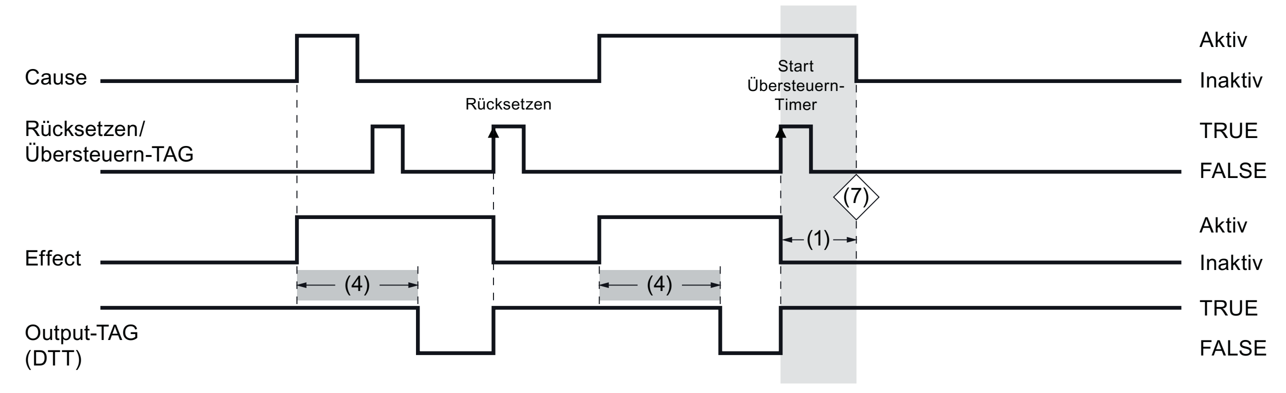
### Rücksetzen/Übersteuern eines Effect mit Ausgabeverzögerung bei Schnittpunkt "V - Übersteuerbar"




- (4), (5), (6): Ausgabeverzögerung-Timer läuft
- (1), (2): Übersteuern-Timer läuft
- (1): Zeit < Maximale Übersteuerungszeit
- (2): Zeit >= Maximale Übersteuerungszeit
- (3): **Alarm**: Zeitüberschreitung beim Übersteuern des Effect; der Alarm wird entweder über eine Bedienung oder durch das nächste Starten des Übersteuern-Timers gelöscht
- (4): Sobald der Effect aktiv wird, wird der Ausgabeverzögerung-Timer gestartet. Nach dessen Ablauf wird dann auch der Output-TAG geändert.
- (5): Der Ausgabeverzögerung-Timer wird auch gestartet, wenn das Übersteuern gestoppt wird bzw. (6) die maximale Übersteuerungszeit überschritten wird.
- Wird der Cause inaktiv, wird auch der Effect inaktiv, unabhängig davon, ob gerade der Ausgabeverzögerung-Timer oder der Übersteuern-Timer läuft.
- Der Übersteuern-TAG hat keine Auswirkung, solange der Ausgabeverzögerung-Timer läuft oder der Cause inaktiv ist.

### Rücksetzen/Übersteuern eines Effect mit Ausgabeverzögerung bei Schnittpunkt "R - Rücksetzbar und Übersteuerbar"



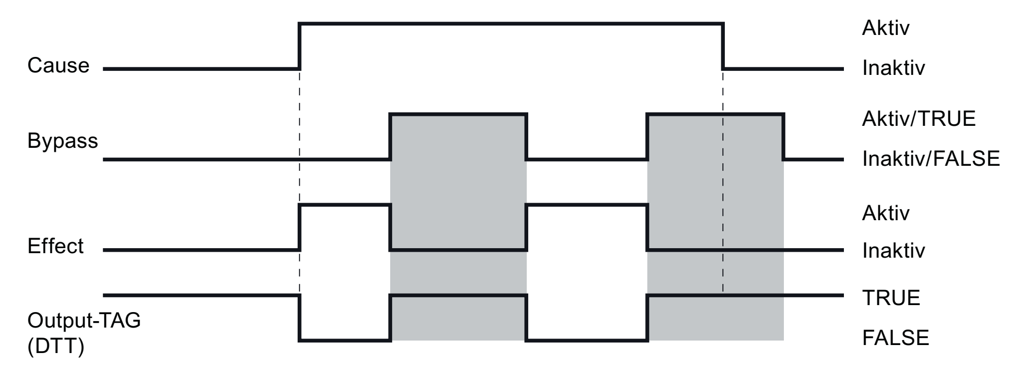

- (4), (5), (6): Ausgabeverzögerung-Timer läuft
- (1), (2): Übersteuern-Timer läuft
- (1): Zeit < Maximale Übersteuerungszeit
- (2): Zeit >= Maximale Übersteuerungszeit
- (3): **Alarm**: Zeitüberschreitung beim Übersteuern des Effect; der Alarm wird entweder über eine Bedienung oder durch das nächste Starten des Übersteuern-Timers gelöscht
- Dieser Schnittpunkt bildet die Kombination aus den Schnittpunkten S und V mit Ausgabeverzögerung, mit der Besonderheit, dass kein Rücksetzen nötig ist, wenn der Übersteuern-Timer beim Inaktivwerden des Cause noch läuft (7).

## 11.2.3 Bypass

### Verhalten beim Bypass in Abhängigkeit zur Projektierung des Schnittpunkts

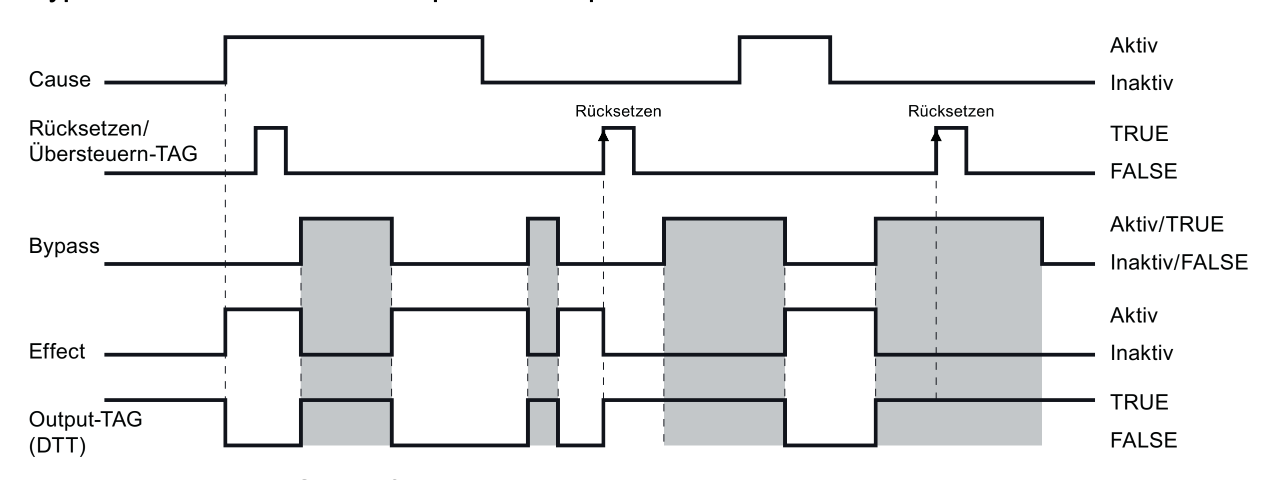
Zusätzlich zum Rücksetzen/Übersteuern-TAG wird nun der Bypass-TAG in die Betrachtung einbezogen.

### Bypass eines Effect bei Schnittpunkt "N - Nicht speichernd"



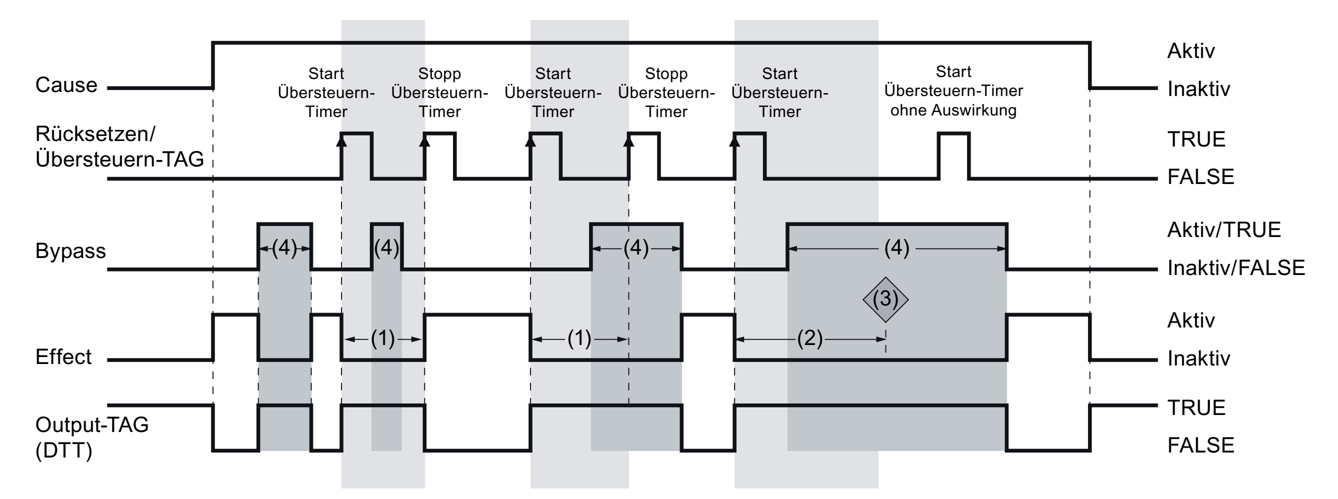

- Graustufe: Bypass aktiv
- Sobald der Bypass aktiv wird, wird der Effect inaktiv. Dies hat bei Schnittpunkt N direkte Auswirkung auf den Output-TAG.
- Wird der Cause inaktiv, hat der Bypass-TAG keine Auswirkungen mehr auf Effect oder Output-TAG.

### Bypass eines Effect bei Schnittpunkt "S - Speichernd"




- Graustufe: Bypass aktiv
- Rücksetzen hat keine Auswirkung, wenn Cause aktiv ist.
- Erst wenn der Cause inaktiv wurde, kann zurückgesetzt werden.
- Ist der Cause inaktiv, hat der Bypass so lange Auswirkung auf die Aktivität des Effect und somit auf den Output-TAG, solange der Effect noch nicht durch eine positive Flanke des Rücksetzen/Übersteuern-TAG zurückgesetzt wurde.

## Bypass eines Effect bei Schnittpunkt "V - Übersteuerbar"




- (1), (2): Übersteuern-Timer läuft
- (4): Bypass aktiv
- (1): Zeit < Maximale Übersteuerungszeit
- (2): Zeit >= Maximale Übersteuerungszeit
- (3): **Alarm**: Zeitüberschreitung beim Übersteuern des Effect; der Alarm wird entweder über eine Bedienung oder durch das nächste Starten des Übersteuern-Timers gelöscht.
- Jeweils eine steigende Flanke des Rücksetzen/Übersteuern-TAG startet und stoppt den Übersteuern-Timer.
- Der Timer wird automatisch gestoppt, sobald die maximale Übersteuerungszeit erreicht wurde (3).
- Wird der Cause inaktiv, so wird auch der Übersteuern-Timer gestoppt.
- Der Übersteuern-Timer wird durch das Aktivieren des Bypass nicht gestoppt.
- Ein gestarteter Übersteuern-Timer kann immer durch eine positive Flanke des Rücksetzen/Übersteuern-TAG wieder gestoppt werden, unabhängig vom Zustand des Bypass.
- Der Übersteuern-Timer kann nicht aktiviert werden, wenn Bypass aktiv ist.



## Bypass eines Effect bei Schnittpunkt "R - Rücksetzbar und Übersteuerbar"

- (1), (2): Übersteuern-Timer läuft
- (4): Bypass aktiv
- (1): Zeit < Maximale Übersteuerungszeit
- (2): Zeit >= Maximale Übersteuerungszeit
- (3): **Alarm**: Zeitüberschreitung beim Übersteuern des Effect; der Alarm wird entweder über eine Bedienung oder durch das nächste Starten des Übersteuern-Timers gelöscht.
- Jeweils eine steigende Flanke des Rücksetzen/Übersteuern-TAG startet und stoppt den Übersteuern-Timer.
- Der Timer wird automatisch gestoppt, sobald die maximale Übersteuerungszeit erreicht wurde (3).
- Wird der Cause inaktiv, so wird auch der Übersteuern-Timer gestoppt.
- Wird der Cause inaktiv während der Übersteuern-Timer läuft, so ist kein Rücksetzen nötig, um den Effect inaktiv zu schalten.
- Der Übersteuern-Timer wird durch das Aktivieren des Bypass nicht gestoppt.

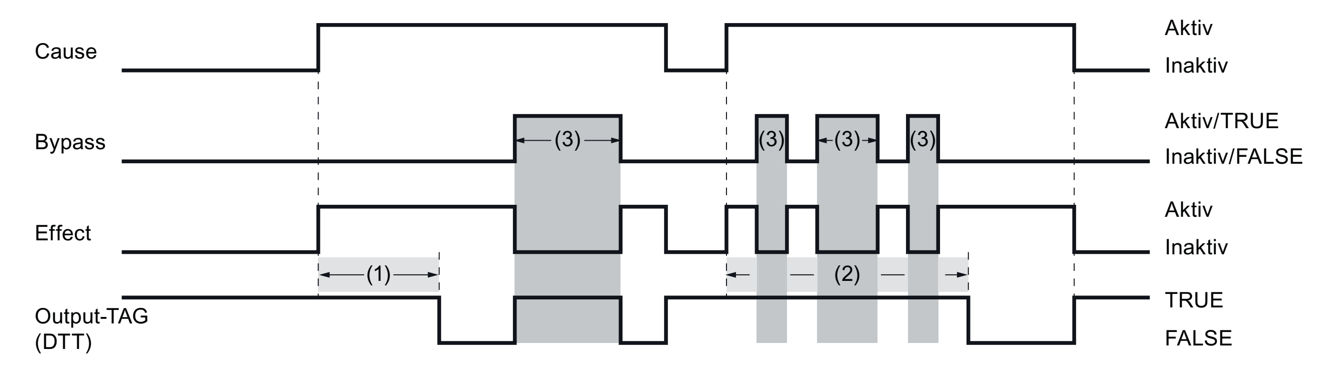
- Ein gestarteter Übersteuern-Timer kann immer durch eine positive Flanke des Rücksetzen/Übersteuern-TAG wieder gestoppt werden, unabhängig vom Zustand des Bypass.
- Der Übersteuern-Timer kann nicht aktiviert werden, wenn Bypass aktiv ist.
- Wenn der Cause inaktiv wurde, kann der Effect durch eine positive Flanke des Rücksetzen/Übersteuern-TAG zurückgesetzt werden.
- Ist der Cause inaktiv, hat der Bypass Auswirkung auf die Aktivität des Effect und somit auf den Output-TAG, solange der Effect noch nicht durch eine positive Flanke des Rücksetzen/Übersteuern-TAG zurückgesetzt wurde.

## 11.2.4 Bypass mit Ausgabeverzögerung

### Verhalten beim Bypass mit Ausgabeverzögerung in Abhängigkeit zur Projektierung des Schnittpunkts

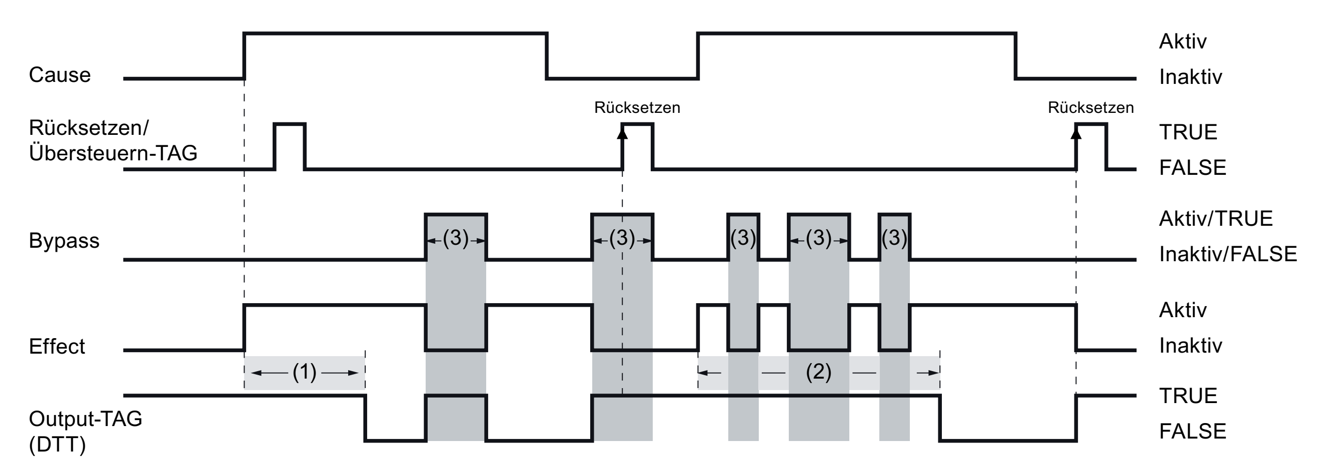
Im Folgenden wird nun der Bypass-TAG mit Ausgabeverzögerung in die Betrachtung einbezogen.

### Bypass eines Effect mit Ausgabeverzögerung bei Schnittpunkt "N - Nicht speichernd"



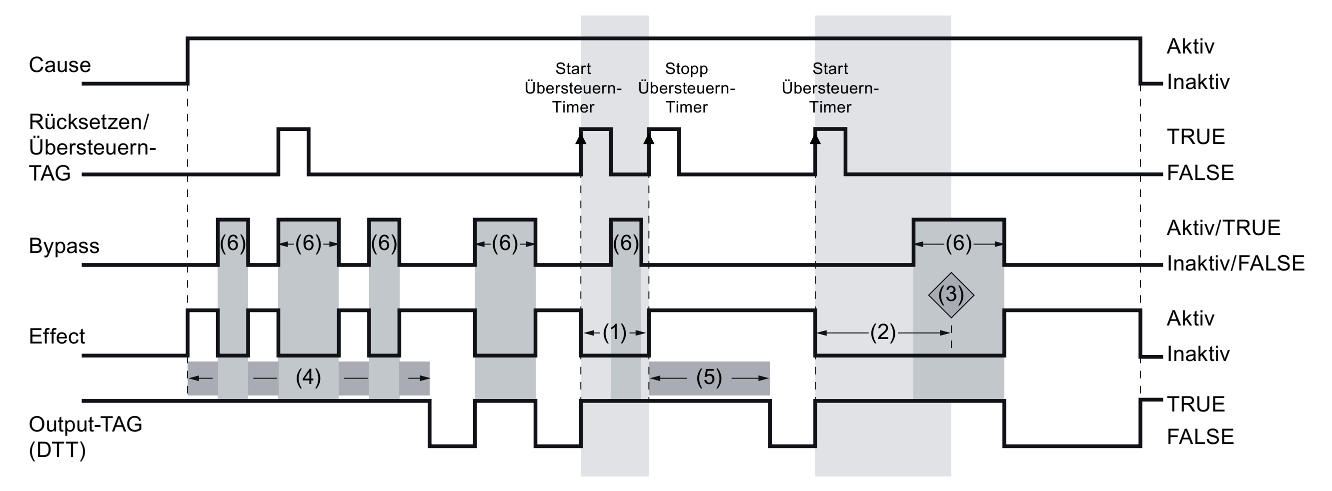

- (1), (2): Ausgabeverzögerung-Timer läuft
- (3): Bypass aktiv
- Wird der Cause inaktiv, so wird auch der Ausgabeverzögerung-Timer gestoppt.
- (2): Bypass unterbricht den Ablauf des Ausgabeverzögerung-Timers. Somit kann die Ausgabeverzögerung zusätzlich verzögert werden.

## Bypass eines Effect mit Ausgabeverzögerung bei Schnittpunkt "S - Speichernd"




- (1), (2): Ausgabeverzögerung-Timer läuft
- (3): Bypass aktiv
- Durch einen aktiven Cause wird der Effect aktiviert. Der Ausgabeverzögerung-Timer wird gestartet. Nach dessen Ablauf wird auch der Output-TAG gesetzt (auf FALSE bei DTT; auf TRUE bei ETT).
- (2): Bypass unterbricht den Ablauf des Ausgabeverzögerung-Timers. Somit kann die Ausgabeverzögerung zusätzlich verzögert werden.
- Der Ausgabeverzögerung-Timer wird nur neu gestartet, wenn der Cause aktiv wurde.
- Nachdem der Cause inaktiv wurde, muss der Effect zurückgesetzt werden, ansonsten bleibt er aktiv und der Bypass kann wirken.

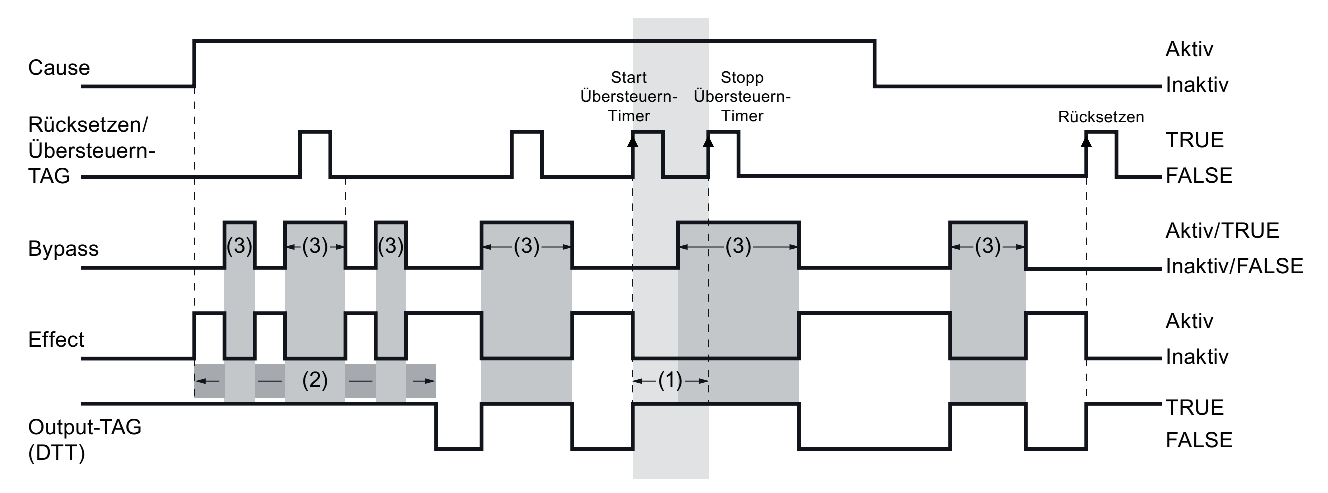
### Bypass eines Effect mit Ausgabeverzögerung bei Schnittpunkt "V - Übersteuerbar"




- (1), (2): Übersteuern-Timer läuft
- (4), (5): Ausgabeverzögerung-Timer läuft
- (6): Bypass aktiv
- (1): Zeit < Maximale Übersteuerungszeit
- (2): Zeit >= Maximale Übersteuerungszeit
- (3): **Alarm**: Zeitüberschreitung beim Übersteuern des Effect; der Alarm wird entweder über eine Bedienung oder durch das nächste Starten des Übersteuern-Timers gelöscht.
- Durch einen aktiven Cause wird der Effect aktiviert. Der Ausgabeverzögerung-Timer wird gestartet. Nach dessen Ablauf wird auch der Output-TAG gesetzt (auf FALSE bei DTT; auf TRUE bei ETT).
- (4): Der Ausgabeverzögerung-Timer kann durch den Bypass unterbrochen werden.
- (4), (5): Der Ausgabeverzögerung-Timer wird nur gestartet, wenn der Cause aktiv wurde oder der Übersteuern-Timer gestoppt wurde und dabei kein Bypass aktiv war.
- Wird der Cause inaktiv, wird der Effect sofort auch inaktiv. Alle Timer werden zurückgesetzt.
- Jeweils eine steigende Flanke des Rücksetzen/Übersteuern-TAG startet und stoppt den Übersteuern-Timer.
- (3): Der Übersteuern-Timer wird gestoppt, sobald die maximale Übersteuerungszeit erreicht wurde.
- (1): Der Übersteuern-Timer wird durch das Aktivieren des Bypass nicht gestoppt.
- Ist der Übersteuern-Timer gestartet und Bypass wird dann aktiviert, kann der Übersteuern-Timer durch eine positive Flanke des Rücksetzen/Übersteuern-TAG wieder gestoppt werden.
- Der Übersteuern-Timer kann nicht aktiviert werden, wenn Bypass aktiv ist.

### Bypass eines Effect mit Ausgabeverzögerung bei Schnittpunkt "R - Rücksetzbar und Übersteuerbar"

Da der Schnittpunkt R eine Kombination aus Schnittpunkt S und V ist, sind auch die Eigenschaften dieser Schnittpunkte hier vertreten.




- (1): Übersteuern-Timer läuft
- (2): Ausgabeverzögerung-Timer läuft
- (3): Bypass aktiv
- Durch einen aktiven Cause wird der Effect aktiviert. Der Ausgabeverzögerung-Timer wird gestartet. Nach dessen Ablauf wird auch der Output-TAG gesetzt (auf FALSE bei DTT; auf TRUE bei ETT).
- (2): Der Ausgabeverzögerung-Timer kann durch den Bypass unterbrochen werden.
- Der Ausgabeverzögerung-Timer wird nur gestartet, wenn der Cause aktiv wurde oder der Übersteuern-Timer gestoppt wurde und dabei kein Bypass aktiv war.
- Jeweils eine steigende Flanke des Rücksetzen/Übersteuern-TAG startet und stoppt den Übersteuern-Timer.
- Der Übersteuern-Timer wird automatisch gestoppt, sobald die maximale Übersteuerungszeit erreicht wurde.
- Der Übersteuern-Timer wird durch das Aktivieren des Bypass nicht beeinflusst.
- Ist der Übersteuern-Timer gestartet und Bypass wird dann aktiviert, kann der Übersteuern-Timer durch eine positive Flanke des Rücksetzen/Übersteuern-TAG wieder gestoppt werden.
- Der Übersteuern-Timer kann nicht aktiviert werden, wenn Bypass aktiv ist.
- Nachdem der Cause inaktiv wurde, muss der Effect zurückgesetzt werden, ansonsten bleibt er aktiv und der Bypass kann wirken.
- Wird der Cause inaktiv, während der Übersteuern-Timer läuft, so wird der Effect nicht gespeichert, d. h. er wird sofort inaktiv und benötigt dazu kein Rücksetzen.
- Wird der Cause inaktiv, während der Ausgabeverzögerung-Timer läuft, wird der Effect gespeichert und erst wieder inaktiv, wenn ein Rücksetzen erfolgte.

## 11.2.5 Prozesswert durchreichen und Maskierungsfreigabe

### Verhalten bei "Prozesswert durchreichen" und Maskierungsfreigabe

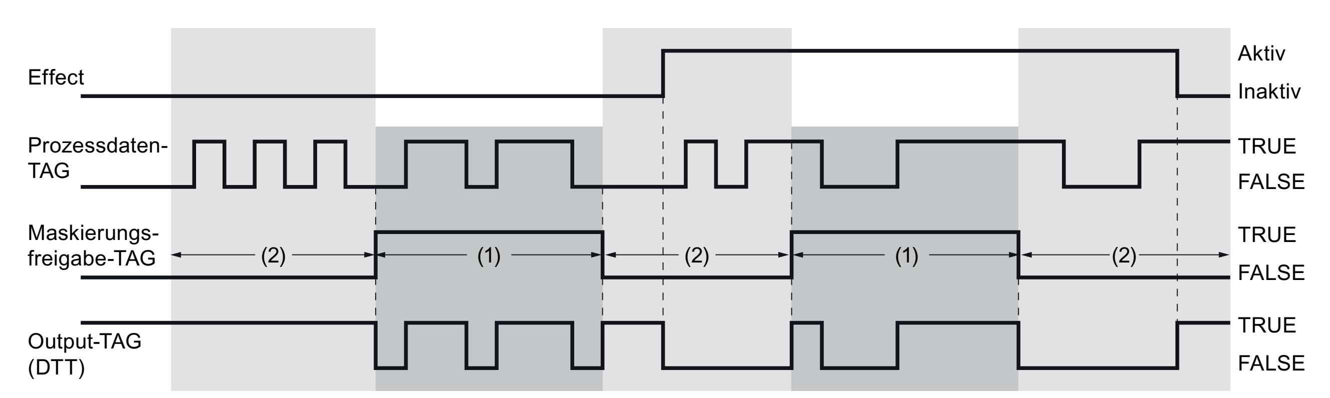
Die Auswirkungen der verschiedenen Kombinationen der beiden Optionen auf die Output-TAGs des Effect werden im Folgenden anhand von Diagrammen näher erläutert.

Tabelle 11- 1 Abhängigkeiten zwischen "Prozesswert durchreichen" und Maskierungsfreigabe

| Prozesswert durchreichen | Maskierungsfreigabe-TAG | Ergebnis |
|---|---|---|
| Nicht aktiviert | Nicht projektiert | Keine Wirkung |
| Nicht aktiviert | Projektiert | Siehe unten: Projektierung "Maskierung" |
| Aktiviert | Nicht projektiert | Siehe unten: Projektierung "Prozesswert durchreichen" |
| Aktiviert | Projektiert | Siehe unten: Projektierung "Prozesswert durchreichen" und "Maskierung" gleichzeitig |

### Projektierung "Maskierung"

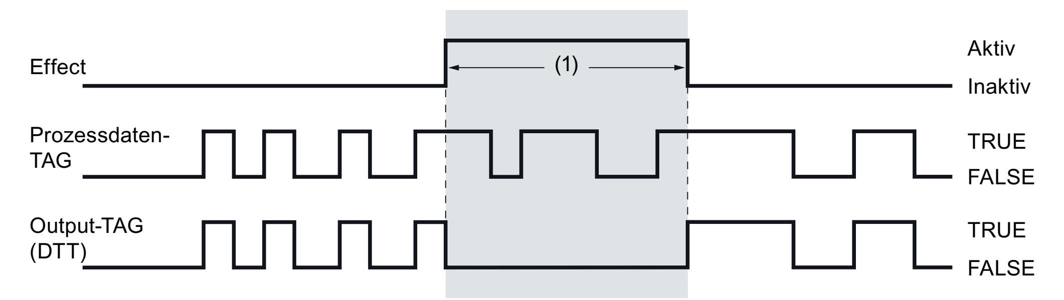
Prozessdaten-TAG und Maskierungsfreigabe-TAG sind projektiert, "Prozesswert durchreichen" ist nicht aktiviert, so folgt der Output-TAG nach folgender Logik:




- Der Wert für den Maskierungsfreigabe-TAG legt fest, ob die Effect-Logik oder eine extern gesteuerte Prozessvariable (der Prozessdaten-TAG) mit den Output-TAGs des Effect verschaltet ist.
- (1): Wenn der Maskierungsfreigabe-TAG TRUE ist, geht der Wert des Prozessdaten-TAG auf die Output-TAGs über.
- (2): Wenn der Maskierungsfreigabe-TAG FALSE ist, wird die Effect-Logik auf die Output-TAGs übernommen.

## Projektierung "Prozesswert durchreichen"

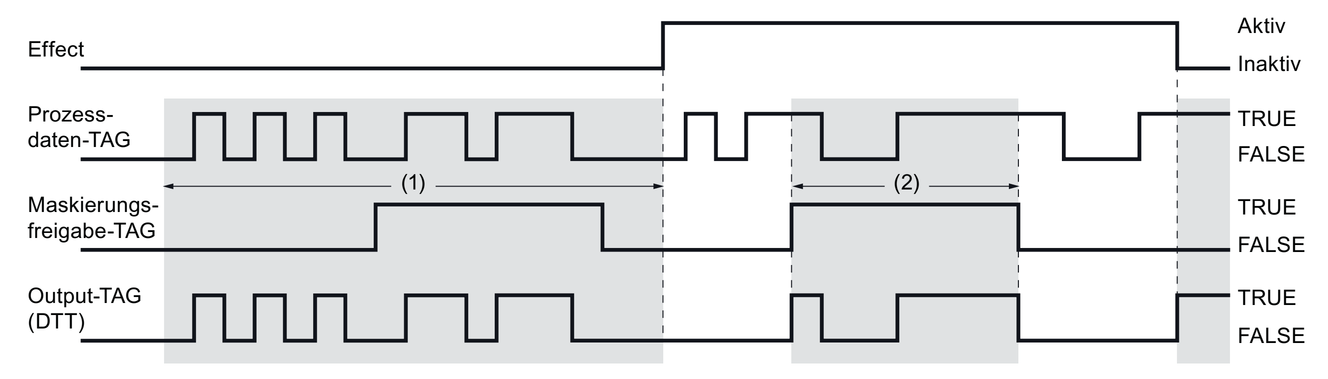
"Prozesswert durchreichen" und Prozessdaten-TAG projektiert, Maskierungsfreigabe-TAG nicht projektiert:




- Das Durchreichen des Prozesswerts wird durch den Zustand des Effect gesteuert.
- Der Wert des Prozessdaten-TAG geht auf die Output-TAGs über, wenn der Effect nicht aktiv ist.
- (1): Wird der Effect aktiv, werden die Output-TAGs durch den Zustand des Effect gesteuert.

## Projektierung "Prozesswert durchreichen" und "Maskierung" gleichzeitig

Prozessdaten-TAG und Maskierungsfreigabe-TAG sind projektiert, "Prozesswert durchreichen" ist aktiviert, so folgt der Output-TAG nach folgender Logik:




- (1): Ist der Effect nicht aktiv, wird immer der Wert des Prozessdaten-TAG auf die Output-TAGs geschaltet, unabhängig vom Wert des Maskierungsfreigabe-TAG.
- (2): Ist der Effect aktiv, wird der Wert des Prozessdaten-TAG nur auf die Output-TAGs geschaltet, wenn der Maskierungsfreigabe-TAG TRUE ist.

# Glossar

## 2-Bediener-Szenario

Bei der Projektierung der Safety Matrix in der PCS 7 OS können Sie ein 2-Bediener-Szenario wählen (4-Augen-Prinzip). Hierfür sind zwei Rollen für Bediener definiert: Initiator und Confirmer.

- Initiator: Der Bediener darf eine Bedienung starten.
- Confirmer: Der Bediener darf eine Bedienung bestätigen.

Die Benutzer müssen zusätzlich zu der Initiator- und/oder Confirmer-Berechtigung die festgelegte Berechtigungsstufe für die jeweils auszuführende Bedienfunktion besitzen.

## Aktiv

Ein Cause oder Effect kann aktiv werden, was bedeutet, dass er ausgelöst wurde.

Ob und wann ein Cause aktiv wird, wird durch die Input-TAGs, den Funktionstyp und die Optionen des Cause bestimmt.

Die Aktivierung eines Effect hängt von der Beziehung (über die Schnittpunkte) zu den Causes und den Optionen des Effect ab. Ist ein Effect aktiv, so werden die Output-TAGs auf "0" bzw. "1" gesetzt, je nach Option für "Energize-to-trip".

## Anwendersicherheitsfunktion

Die -> Sicherheitsfunktion für den Prozess kann durch eine Anwendersicherheitsfunktion oder eine -> Fehlerreaktionsfunktion erbracht werden. Der Anwender programmiert nur die Anwendersicherheitsfunktion. Wenn das -> F-System im Fehlerfall die eigentliche Anwendersicherheitsfunktion nicht mehr ausführen kann, führt es die Fehlerreaktionsfunktion aus: z. B. werden die zugehörigen Ausgänge abgeschaltet und ggf. geht die -> F-CPU in STOP.

## Cause

Ein Cause ( = Ursache) repräsentiert ein Prozessereignis.

Der Cause bildet die Ursache für die Aktivierung eines Effect. Es müssen bestimmte Bedingungen erfüllt sein, damit der Cause aktiv wird und somit über einen Schnittpunkt auf einen Effect wirkt.

Als Input-Typ stehen analoge oder diskrete Werte zur Auswahl. Die Werte von mindestens einem und maximal drei Input-TAGs bilden zusammen über den Funktionstyp einen Cause.

## CRC

Cyclic Redundancy Check -> Prüfwert CRC

## Deaktivierter Sicherheitsbetrieb

Zeitweises Ausschalten des -> Sicherheitsbetriebs für Testzwecke, Inbetriebsetzung, etc.

Während des deaktivierten Sicherheitsbetriebs muss die Sicherheit der Anlage durch andere organisatorische Maßnahmen, z. B. beobachteter Betrieb und manuelle Sicherheitsabschaltung, sichergestellt werden.

## Deenergize-to-trip (DTT)

Auslösen bei FALSE: Der Cause ist aktiv, wenn Input-TAG = "0" (low-active). Der Output-TAG ist "0", wenn der Effect aktiv ist. Diese negative Logik ist die Standardeinstellung für die Eingänge und Ausgänge der Safety Matrix.

## Depassivierung

-> Wiedereingliederung

## Effect

Ein Effect ( = Wirkung) repräsentiert die Reaktion der Safety Matrix, die sie auf den Prozess ausübt.

Es müssen bestimmte Bedingungen erfüllt sein, damit der Effect aktiv wird und somit über seine Output-TAGs auf den Prozess wirkt.

Die Werte von mindestens einem und maximal vier diskreten Output-TAGs bilden die Wirkung auf den Prozess. Die Aktivierung eines Effect hängt von verschiedenen Faktoren ab (Zustand der zugeordneten Causes, Typ des Schnittpunkts, eingestellte Optionen des Effect).

## Energize-to-trip (ETT)

Auslösen bei TRUE: Der Cause ist aktiv, wenn Input-TAG = "1" (high-active). Der Output-TAG ist "1", wenn der Effect aktiv ist.

## ES

Engineering System (ES): Projektiersystem, mit dem auf komfortable, visuelle Weise das Prozessleitsystem an die gestellten Aufgaben angepasst wird.

## F-Ablaufgruppe

Bei der Programmierung des -> Sicherheitsprogramms dürfen die -> F-Bausteine nicht direkt in Tasks/OBs, sondern müssen in F-Ablaufgruppen eingefügt werden. Das Sicherheitsprogramm besteht aus mehreren F-Ablaufgruppen.

## F-Abschaltgruppen

F-Abschaltgruppen enthalten eine oder mehrere -> F-Ablaufgruppen. F-Ablaufgruppen-Kommunikationsbausteine zwischen den -> F-Bausteinen in verschiedenen F-Ablaufgruppen, die alle einer F-Abschaltgruppe zugeordnet sind, sind nicht erforderlich. Wird ein Fehler in einer F-Abschaltgruppe erkannt, so wird diese F-Abschaltgruppe abgeschaltet, die Abschaltung weiterer F-Abschaltgruppen ist von der Projektierung des F_SHUTDN abhängig.

## F-Anlauf

Bei einem F-Anlauf handelt es sich um einen Restart nach einem F-STOP oder STOP der F-CPU. *S7 F Systems* unterscheidet nicht zwischen dem Kaltstart und Warmstart der F-CPU.

## F-Bausteine

Als F-Bausteine werden alle F-Bausteine bezeichnet:

- die vom Anwender aus einer F-Bibliothek ausgewählt werden
- die automatisch im -> Sicherheitsprogramm ergänzt werden

## F-Bausteintyp

F-Bausteintypen sind vorgefertigte Programmteile, die in einen CFC-Plan verwendet werden können (z.B. fehlersicherer Additionsbaustein F_ADD_R, fehlersicherer Multiplexer F_MUX2_R usw.). Beim Einfügen werden Bausteininstanzen erzeugt. Von einem F-Bausteintyp können beliebig viele Bausteininstanzen angelegt werden.

Der F-Bausteintyp legt die Charakteristik (Algorithmus) für alle Verwendungen dieses Typs fest. Der Name des F-Bausteintyps wird in der Symboltabelle festgelegt.

## F-CPU

Eine F-CPU ist eine F-fähige Zentralbaugruppe, die für den Einsatz in *S7 F Systems* zugelassen ist. Für *S7 F Systems* erlaubt die F-Runtime-Lizenz dem Anwender, die Zentralbaugruppe als F-CPU einzusetzen, d. h. ein -> Sicherheitsprogramm darin ablaufen zu lassen. In der F-CPU kann außerdem ein -> Standard-Anwenderprogramm ablaufen.

## F-Datentyp

Standard-Anwenderprogramm und -> Sicherheitsprogramm benutzen unterschiedliche Datenformate. Im Sicherheitsprogramm werden sicherheitsgerichtete F-Datentypen verwendet.

## Fehlerreaktionsfunktion

-> Anwendersicherheitsfunktion

## Fehlersichere Systeme

Fehlersichere Systeme (F-Systeme) sind dadurch gekennzeichnet, dass sie beim Auftreten bestimmter Ausfälle im -> sicheren Zustand bleiben oder unmittelbar in einen anderen sicheren Zustand übergehen.

## Fehlertoleranzzeit

Die Fehlertoleranzzeit eines Prozesses ist das Zeitintervall, innerhalb dessen der Prozess sich selbst überlassen bleiben kann, ohne dass Schaden für Leib und Leben des Bedienungspersonals oder für die Umwelt entsteht.

Innerhalb der Fehlertoleranzzeit kann das den Prozess steuernde -> F-System beliebig steuern, d. h. auch falsch oder gar nicht. Die Fehlertoleranzzeit eines Prozesses hängt von der Art des Prozesses ab und muss individuell ermittelt werden.

## F-Peripherie

Sammelbezeichnung für fehlersichere Ein- und Ausgaben, die in *SIMATIC S7* für die Einbindung in u. a. *S7 F Systems* zur Verfügung stehen. Es stehen für *S7 F Systems* zur Verfügung:

- fehlersichere Peripheriemodule ET 200eco
- fehlersichere Signalbaugruppen S7-300 (-> F-SMs)
- fehlersichere Module ET 200pro
- fehlersichere Module für ET 200S
- fehlersichere DP-Normslaves
- fehlersichere PA-Feldgeräte

## F-SMs

Fehlersichere Signalbaugruppen des S7-300-Baugruppenspektrums, die für den sicherheitsgerichteten Betrieb (-> Sicherheitsbetrieb) zentral in einer S7 300 oder im dezentralen Peripheriesystem ET 200M eingesetzt werden können. Die F-SMs sind mit integrierten -> Sicherheitsfunktionen ausgestattet.

## F-Systeme

Fehlersichere Systeme

## F-Zykluszeit

Weckalarmzeit für OBs mit -> F-Ablaufgruppen

## Gesamtsignaturen

Die Gesamtsignaturen kennzeichnen eindeutig einen bestimmten Stand des -> Sicherheitsprogramms. Sie sind wichtig für die Vorortabnahme des Sicherheitsprogramms, z. B. durch Sachverständige.

## Inaktiv

Ein Cause oder Effect kann inaktiv werden, was bedeutet, die Bedingungen für die Aktivierung sind nicht erfüllt.

Ob der Cause inaktiv wird, wird durch die Input-TAGs, den Funktionstyp und die Optionen des Cause bestimmt.

Die Deaktivierung eines Effect hängt von der Beziehung (über die Schnittpunkte) zu den Causes und den Optionen des Effect ab. Ist ein Effect inaktiv, so werden die Output-TAGs auf "0" bzw. "1" gesetzt, je nach Option für "Energize-to-trip".

## Initiator/Confirmer

Wenn die Transaktion für die Bedienung einer Safety Matrix von zwei Bedienern durchgeführt wird, legen Sie zwei Benutzer an:

- Der Initiator startet die Bedienung einer Safety Matrix über Secure Write. Dieser Benutzer muss die Berechtigung besitzen, die dem Attribut "InitiatorLevel" in den Eigenschaften des Bausteinsymbols zugewiesen ist. Der Initiator besitzt jedoch nicht die Berechtigung, die Bedienung zu bestätigen.
- Der Confirmer überprüft und bestätigt die Bedienung. Dieser Benutzer muss die Berechtigung besitzen, die dem Attribut "ConfirmerLevel" in den Eigenschaften des Bausteinsymbols zugewiesen ist. Der Confirmer besitzt jedoch nicht die Berechtigung, die Bedienung zu starten.

## Kanalfehler

kanalbezogener Fehler, z. B. Drahtbruch oder Kurzschluss

## Kategorie

Kategorie nach EN 954-01

Mit *S7 F Systems* ist im -> Sicherheitsbetrieb der Einsatz bis Kategorie 4 möglich.

## OS

**O**perator **S**tation (OS): Projektierbare Bedienstation zur Bedienung und Überwachung von Maschinen und Anlagen.

## Passivierung

Passivierung digitaler Ausgabekanäle bedeutet, dass die Ausgänge in den strom- oder spannungslosen Zustand gebracht werden.

Die Passivierung digitaler Eingabekanäle findet statt, wenn die Eingänge (über die fehlersicheren Treiber) einen Wert "0" an die F-CPU übertragen, unabhängig vom aktuellen Prozesssignal.

Die Passivierung analoger Eingabekanäle findet statt, wenn die Eingänge (über die fehlersicheren Treiber) einen Ersatzwert oder den zuletzt gültigen Wert an die F-CPU übertragen, unabhängig vom aktuellen Prozesssignal.

## PROFIsafe

Sicherheitsgerichtetes Busprofil von PROFIBUS DP/PA und PROFINET IO für die Kommunikation zwischen dem -> Sicherheitsprogramm und der -> F-Peripherie in einem -> F-System.

## Proof-Test-Intervall

Zeitraum, nach welchem eine Komponente in den fehlerfreien Zustand versetzt werden muss, d. h., sie wird durch eine unbenutzte Komponente ersetzt oder ihre vollständige Fehlerfreiheit wird nachgewiesen.

## Prüfwert CRC

Die Gültigkeit der im -> Sicherheitstelegramm enthaltenen Prozesswerte, die Korrektheit der zugeordneten Adressbeziehungen und die sicherheitsrelevanten Parameter werden über einen im -> Sicherheitstelegramm enthaltenen Prüfwert CRC abgesichert.

## *S7-PLCSIM*

Mit *S7-PLCSIM* können Sie Ihr S7-Programm auf einem simulierten Automatisierungssystem, das auf Ihrem ES/OS existiert, bearbeiten und testen. Da die Simulation vollständig in STEP 7 realisiert wird, benötigen Sie keine Hardware (CPU, F-CPU, Peripherie).

## Schnittpunkt

Schnittpunkte bilden die Verknüpfung zwischen Cause und Effect.

## Sicherer Zustand

Grundlage des Sicherheitskonzepts in -> fehlersicheren Systemen ist, dass für alle Prozessgrößen ein sicherer Zustand existiert. Bei digitaler -> F-Peripherie ist das immer der Wert "0".

## Sicherheitsbetrieb

1. Betriebsart von -> F-Peripherie, in der -> sicherheitsgerichtete Kommunikation über -> Sicherheitstelegramme möglich ist.
2. Betriebsart des Sicherheitsprogramms. Im Sicherheitsbetrieb des Sicherheitsprogramms sind alle Sicherheitsmechanismen zur Fehlererkennung und Fehlerreaktion aktiviert. In diesem Zustand ist eine Änderung des Sicherheitsprogramms im laufenden Betrieb nicht möglich. Der Sicherheitsbetrieb kann vom Anwender deaktiviert werden (-> deaktivierter Sicherheitsbetrieb).

## Sicherheitsfunktion

In -> F-CPU und -> F-Peripherie integrierter Mechanismus, der den Einsatz in -> fehlersicheren Systemen ermöglicht.

Nach IEC 61508: Funktion, die von einer Sicherheitseinrichtung implementiert wird, um im Fall eines bestimmten Fehlers das System im -> sicheren Zustand zu halten oder es in einen sicheren Zustand zu bringen (-> Anwendersicherheitsfunktion).

## Sicherheitsgerichtete Kommunikation

Kommunikation, die dem Austausch von fehlersicheren Daten dient.

## Sicherheitsklasse

Sicherheits-Integritätslevel (Safety Integrity Level) SIL nach IEC 61508. Je höher der Safety Integrity Level ist, desto schärfer sind die Maßnahmen zur Vermeidung systematischer Fehler, sowie zur Beherrschung von systematischen Fehlern und zufälligen Hardware-Ausfällen.

Mit *S7 F Systems* ist im Sicherheitsbetrieb der Einsatz bis Sicherheitsklasse SIL3 möglich.

## Sicherheitsprogramm

Sicherheitsgerichtetes Anwenderprogramm

## Sicherheitsprotokoll

-> Sicherheitstelegramm

## Sicherheitstechnische Funktionsgruppen (SIF)

Sicherheitstechnische Funktionsgruppen (Safety Instrumented Function groups) können Sie nach Maßgabe Ihrer Anwendung selbst anlegen, d. h. Sie unterteilen Ihre Anwendung in Funktionsgruppen, die Sie dann im *Safety Matrix Engineering Tool* und *Safety Matrix Viewer* gezielt beobachten und ändern können (z. B. "Füllstandsmessung und Abschaltung").

Um diese Funktion nutzen zu können, müssen Sie die einzelnen Causes und Effects des Sicherheitsprogramms Ihren Sicherheitstechnischen Funktionsgruppen zuordnen. Dann können Sie einzelne, mehrere oder alle Sicherheitstechnischen Funktionsgruppen anzeigen.

## Sicherheitstelegramm

Im -> Sicherheitsbetrieb werden die Daten zwischen -> F-CPU und -> F-Peripherie bzw. bei sicherheitsgerichteter CPU-CPU-Kommunikation zwischen den F-CPUs in einem Sicherheitstelegramm übertragen.

## Signatur

-> Gesamtsignaturen

## Standard-Anwenderprogramm

nicht sicherheitsgerichtetes Anwenderprogramm

## Standardbetrieb

Betriebsart von -> F-Peripherie, in der keine -> sicherheitsgerichtete Kommunikation über -> Sicherheitstelegramme möglich ist, sondern nur -> Standard-Kommunikation.

## Standard-Kommunikation

Kommunikation, die dem Austausch von nicht sicherheitsgerichteten Daten dient.

## Teilabschaltung

Nur die F-Abschaltgruppe wird abgeschaltet, in der der Fehler erkannt wurde.

## Wiedereingliederung

Die Umschaltung von Ersatzwerten (0) auf Prozesswerte (Wiedereingliederung einer F-Peripherie) erfolgt automatisch oder erst nach einer Anwenderquittierung am F-Kanaltreiber.

Diese Art der Wiedereingliederung ist abhängig:

- von der Ursache für die Passivierung der F-Peripherie/der Kanäle der F-Peripherie
- von einer Parametrierung am F-Kanaltreiber

Nach einer Wiedereingliederung werden bei einer F-Peripherie mit Eingängen wieder die an den fehlersicheren Eingängen anstehenden Prozesswerte am Ausgang des F-Kanaltreibers bereitgestellt. Bei einer F-Peripherie mit Ausgängen werden vom F-System wieder die am Eingang des F-Kanaltreibers anliegenden Ausgabewerte zu den fehlersicheren Ausgängen übertragen.

## Zugriffschutz

-> Fehlersichere Systeme müssen vor gefährlichem, unerlaubtem Zugriff geschützt werden. Der Zugriffschutz für F-Systeme wird realisiert durch die Vergabe von zwei Passwörtern (für die -> F-CPU und für das -> Sicherheitsprogramm).

# Index

## T



## U



## V



## W



## Z